

SET-THEORETIC SOLUTIONS OF THE YANG–BAXTER EQUATION, RC-CALCULUS, AND GARSIDE GERMS

PATRICK DEHORNOY

ABSTRACT. Building on a result by W. Rump, we show how to exploit the right-cyclic law $(xy)(xz) = (yx)(yz)$ in order to investigate the structure groups and monoids attached with (involutive nondegenerate) set-theoretic solutions of the Yang–Baxter equation. We develop a sort of right-cyclic calculus, and use it to obtain short proofs for the existence both of the Garside structure and of the I -structure of such groups. We describe finite quotients that play for the considered groups the role that Coxeter groups play for Artin–Tits groups.

The Yang–Baxter equation (YBE) is a fundamental equation occurring in integrable models in statistical mechanics and quantum field theory [26]. Among its many solutions, some simple ones called set-theoretic turn out to be connected with several interesting algebraic structures. In particular, a group and a monoid are attached with every set-theoretic solution of YBE [16], and the family of all groups and monoids arising in this way is known to have rich properties: as shown by T. Gateva–Ivanova and M. Van den Bergh in [20] and by E. Jespers and J. Okniński in [24], they admit an I -structure, meaning that their Cayley graph is isometric to that of a free Abelian group, and, as shown by F. Chouraqui in [5], they admit a Garside structure, (roughly) meaning that they are groups of fractions of monoids in which divisibility relations are lattice orders.

It was shown by W. Rump in [27] that (involutive nondegenerate) set-theoretic solutions of YBE are in one-to-one correspondence with algebraic structures consisting of a set equipped with a binary operation $*$ that obeys the right-cyclic law $(xy)(xz) = (yx)(yz)$ and has bijective left-translations. In this paper, we merge the ideas stemming from the right-cyclic law (RC-law) and those coming from Garside theory to give easy alternative proofs of earlier results and derive new results. The key technical point is the connection between the RC-law and the least common right-multiple operation. A nice point is that one never needs to restrict to squarefree solutions of YBE, that is, those satisfying $\rho(s, s) = (s, s)$.

The main benefit of the current approach is to provide a simple and complete solution to the problem of finding a *Garside germ* for every group associated with a set-theoretic solution of YBE, namely finding a finite quotient of the group that encodes the whole structure in the way a finite Coxeter group encodes the associated Artin–Tits group. The precise statement (Proposition 5.2) says that, if $(S, *)$ is an RC-quasigroup with cardinality n and class d (a certain numerical parameter attached with every finite RC-quasigroup), then starting from the canonical presentation of the associated group and adding the RC-torsion relations $s^{[d]} = 1$

2010 *Mathematics Subject Classification.* 20F38, 20N02, 20M10, 20F55, 06F05, 16T25.

Key words and phrases. Yang–Baxter equation, set-theoretic solution, Garside monoid, Garside group, monoid of I -type, right-cyclic law, RC-quasigroup, birack.

with s in S (where $s^{[d]}$ is a sort of twisted d th power) provides a finite group \overline{G} of order d^n from which the Garside structure of G can be retrieved. Partial results corresponding to class 2, namely RC-quasigroups satisfying $(xx)(xy) = y$, are established by hand in [6]. Our current approach based on RC-calculus and the I -structure enables one to address the general case directly.

The above finite “Coxeter-like” group \overline{G} does not coincide (in general) with the finite quotient G_X^0 considered in [16] and called involutive Yang–Baxter group (IYB) in [3, 4]: the latter is a (proper) quotient of the group \overline{G} (see Remark 5.9(ii)) and, contrary to \overline{G} , it does not fully encode the situation since many different solutions may be associated with the same IYB group [3].

No exhaustive description of Coxeter-like groups is known so far, but it is easy to characterize them as those finite groups that admit a “modular I -structure”, namely the counterpart of an I -structure where the free Abelian group \mathbb{Z} is replaced with a cyclic group $\mathbb{Z}/d\mathbb{Z}$ (Proposition 5.10), a special case of the notion of IG-structure considered in [23]. If \overline{G} is associated with a cardinal n RC-quasigroup, its Cayley graph is naturally drawn on an n -torus, and \overline{G} can be realized as a group of isometries in an n -dimensional Hermitian space (Corollary 5.15). We hope that further properties will be discovered soon.

The paper is organized as follows. In Section 1, we recall the connection between set-theoretic solutions of the Yang–Baxter equation and algebraic systems that obey the RC-law and introduce the derived structure monoids and groups. In Section 2, we establish various consequences of the RC-law which altogether make a sort of right-cyclic calculus. In Section 3, this calculus is used to investigate the divisibility relations of the monoids associated with RC-quasigroups and their Garside structure. Then, in Section 4 (which is mostly independent from Section 3), we use the RC-calculus to similarly investigate the I -structure. Finally, in Section 5, we merge the results to construct a finite quotient that encodes the whole structure and give several descriptions of this “Coxeter-like” group, in particular as a group of isometries of an Hermitian space.

ACKNOWLEDGMENTS

The author wishes to thank Tatiana Gateva-Ivanova, Eddy Godelle, Eric Jespers, Gilbert Levitt, Jan Okniński, and, specially, Wolfgang Rump for discussions about the content of this paper.

1. SEVERAL EQUIVALENT FRAMEWORKS

In this introductory section, we recall the definition of set-theoretic solutions of the Yang–Baxter equation [16] and their connection with what we shall call *RC-quasigroups*, which are sets equipped with a binary operation obeying the right-cyclic law $(x * y) * (x * z) = (y * x) * (y * z)$, as established by W. Rump in [27].

Definition 1.1. [15, 16] A *set-theoretic solution of YBE* (or *braided quadratic set*) is a pair (S, ρ) where S is a set and ρ is a bijection of $S \times S$ into itself that satisfies

$$(1.1) \quad \rho^{12} \rho^{23} \rho^{12} = \rho^{23} \rho^{12} \rho^{23}.$$

where ρ^{ij} is the map of S^3 to itself obtained when ρ acts on the i th and j th entries.

If (S, ρ) is a set-theoretic solution of YBE and V is a vector space based on S , then the (unique) linear operator R on $V \otimes V$ that extends ρ is a solution of the (non-parametric, braid form of) the Yang–Baxter equation $R^{12}R^{23}R^{12} = R^{23}R^{12}R^{23}$, and, conversely, every solution of YBE such that there exists a basis S of the ambient vector space such that $S^{\otimes 2}$ is globally preserved is of this type.

A set-theoretic solution (S, ρ) of YBE is called *nondegenerate* if, writing $\rho_1(s, t)$ and $\rho_2(s, t)$ for the first and second entries of $\rho(s, t)$, the left-translation $y \mapsto \rho_1(s, y)$ is one-to-one for every s in S and the right-translation $x \mapsto \rho_2(x, t)$ is one-to-one for every t in S . A solution (S, ρ) is called *involutive* if $\rho \circ \rho$ is the identity of $S \times S$.

A map from $S \times S$ to itself is a pair of maps from $S \times S$ to S , hence a pair of binary operations on S . Translating into the language of binary operations the constraints that define set-theoretic solutions of YBE is straightforward.

Lemma 1.2. *Define a birack to be an algebraic system (S, \rfloor, \lceil) consisting of a set S equipped with two binary operations \rfloor and \lceil that satisfy*

$$(1.2) \quad (a \rfloor b) \rfloor ((a \lceil b) \lceil c) = a \rfloor (b \lceil c),$$

$$(1.3) \quad (a \rfloor b) \lceil ((a \lceil b) \rfloor c) = (a \lceil (b \rfloor c)) \rfloor (b \lceil c),$$

$$(1.4) \quad (a \lceil b) \rfloor c = (a \lceil (b \rfloor c)) \rfloor (b \lceil c),$$

and are such that the left-translations of \rfloor and the right-translations of \lceil are one-to-one, and call a birack involutive if it satisfies in addition

$$(1.5) \quad (a \rfloor b) \rfloor (a \lceil b) = a \quad \text{and} \quad (a \rfloor b) \lceil (a \lceil b) = b.$$

(i) *If (S, ρ) is a nondegenerate set-theoretic solution of YBE, then defining $a \rfloor b = \rho_1(a, b)$ and $a \lceil b = \rho_2(a, b)$ yields a birack (S, \rfloor, \lceil) . If (S, ρ) is involutive, then the birack (S, \rfloor, \lceil) is involutive.*

(ii) *Conversely, if (S, \rfloor, \lceil) is a birack, then defining $\rho(a, b) = (a \rfloor b, a \lceil b)$ yields a nondegenerate set-theoretic solution (S, ρ) of YBE. If the birack (S, \rfloor, \lceil) is involutive, then (S, ρ) is involutive.*

Lemma 1.2 appears as Remark 1.6 in [21], using the notation $({}^a b, a^b)$ for $(a \rfloor b, a \lceil b)$. Biracks appeared in low-dimensional topology as a natural algebraic counterpart of Reidemeister move III [17]. If $a \lceil b = a$ always holds, (1.2)–(1.4) reduce to the left-selfdistributivity law $(a \rfloor b) \rfloor (a \rfloor c) = a \rfloor (b \rfloor c)$, corresponding, when left-translations are bijective, to (S, \rfloor) being a rack [18]. Note that a birack obtained from a rack is involutive only if $s \rfloor t = t$ holds for all s, t (trivial birack).

Thus, investigating involutive nondegenerate set-theoretic solutions of YBE and involutive biracks are equivalent tasks. We now make a second step following [27]. If \rfloor is a binary operation on S and its left-translations are one-to-one, defining $a * b$ to be the unique c satisfying $a \rfloor c = b$ provides a well-defined binary operation on S , which can be viewed as a left-inverse of \rfloor . The seminal observation of [27] is that, if (S, \rfloor, \lceil) is a birack, then the left-inverse $*$ of the operation \rfloor obeys a simple algebraic law and the whole structure can be recovered from that operation $*$.

Definition 1.3 (Rump [27]). *A right-cyclic system, or RC-system, is a pair $(S, *)$ where $*$ is a binary operation on the set S that obeys the right-cyclic law RC*

$$(1.6) \quad (x * y) * (x * z) = (y * x) * (y * z).$$

An *RC-quasigroup* is an RC-system whose left-translations are one-to-one, that is, for every s in S , the map $t \mapsto s * t$ is one-to-one. An RC-system is called *bijective* if the map $(s, t) \mapsto (s * t, t * s)$ is a bijection of $S \times S$ to itself.

In [27], RC-systems are called “cycloids” and RC-quasigroups are called “cycle sets”; the current terminology may seem convenient in view of subsequent variants (and the widely used convention that “quasigroup” refers to bijective translations).

Example 1.4. Every operation $s * t = f(t)$ with f a permutation of S provides a (semi-trivial) bijective RC-quasigroup. Another example (important in Section 3 below) is the right-complement operation in a monoid: if M is a left-cancellative monoid in which any two elements admit a unique least common right-multiple, then the operation \setminus such that $f(f \setminus g)$ is the least common right-multiple of f and g obeys (1.6), as easily follows from the commutativity and associativity of the right-lcm. So (M, \setminus) is an RC-system (but, in general, not an RC-quasigroup).

The following result, which is essentially [27, Prop. 1] shows that the context of a bijective RC-quasigroup is entirely equivalent to that of an involutive nondegenerate set-theoretic solution of the YBE.

Proposition 1.5. (i) *Assume that (S, ρ) is an involutive nondegenerate set-theoretic solution of YBE. For s, t in S , define $s * t$ to be the unique r satisfying $\rho_1(s, r) = t$. Then $(S, *)$ is a bijective RC-quasigroup.*

(ii) *Conversely, assume that $(S, *)$ is a bijective RC-quasigroup. For a, b in S , define $\rho(a, b)$ to be the unique pair (a', b') satisfying $a * a' = b$ and $a' * a = b'$. Then (S, ρ) is an involutive nondegenerate set-theoretic solution of YBE.*

As the result essentially appears in [27], we shall not go into the details of the proof, whose principle is clear: according to Lemma 1.2, the point is to go from the birack laws to the RC-law and *vice versa*, and it consists in repeatedly using the fact that, for all x, y, z in the considered set S , the relation $y = x \rfloor z$ is equivalent to $x * y = z$ and it implies $y * x = x \lceil z$ (for (i)) and, symmetrically, that $z = x * y$ is equivalent to $x \rfloor z = y$ and it implies $x \lceil z = y * x$ (for (ii)). The argument then amounts to completing the cube displayed in Figure 3, where a square diagram

$$\begin{array}{ccc} & \xrightarrow{a'} & \\ a \downarrow & \square & \downarrow b' \\ & \xrightarrow{b} & \end{array}$$
 means that we have $a' = a \rfloor b$ and $b' = a \lceil b$, that is, equivalently, $b = a * a'$ and $b' = a' * a$. As observed by W. Rump, this picture illustrates the nature of (1.6) as a (discrete form of) an integrability condition.

The (small) miracle in Proposition 1.5 is that it reduces the constraints of a birack, which involve two operations and three laws, to those of an RC-quasigroup, which only involves one operation and one law. Actually, a second, symmetric operation is also present in every bijective RC-quasigroup.

Definition 1.6. An *RLC-system* is a triple $(S, *, \tilde{*})$ such that $(S, *)$ is an RC-system, $\tilde{*}$ is a second binary operation on S that obeys the *left-cyclic law LC*

$$(1.7) \quad (z \tilde{*} x) \tilde{*} (y \tilde{*} x) = (z \tilde{*} y) \tilde{*} (x \tilde{*} y),$$

and both operations are connected by

$$(1.8) \quad (y * x) \tilde{*} (x * y) = x = (y \tilde{*} x) * (x \tilde{*} y).$$

An *RLC-quasigroup* is an RLC-system $(S, *, \tilde{*})$ such that the left-translations of $*$ and the right-translations of $\tilde{*}$ are one-to-one.

Then RLC-quasigroups and bijective RC-quasigroups are equivalent structures.

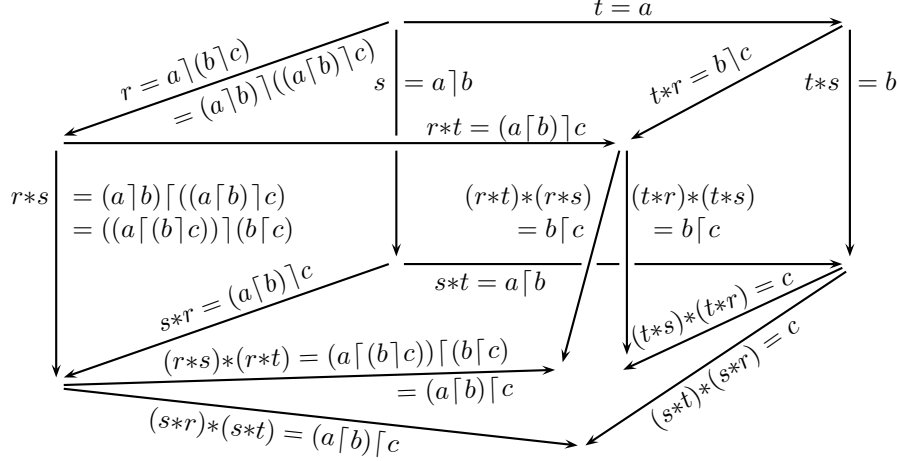


FIGURE 1. Proof of Proposition 1.5(i): one successively evaluates the edges of the cube in terms of a, b, c and the relations (1.2)–(1.4) guarantee that the cube closes. The same diagram can be used for the proof of (ii) below, except that one starts with a closed cube and evaluates some edges in two different ways to establish (1.2)–(1.4).

Lemma 1.7. *For all binary operations $*$, $\tilde{*}$ on a set S , the following are equivalent:*

- (i) *The system $(S, *, \tilde{*})$ obeys the involutivity laws (1.8).*
- (ii) *The map $\Psi : (s, t) \mapsto (s * t, t * s)$ is a bijection of $S \times S$ to itself and $\tilde{*}$ is the unique operation on S such that the map $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is the inverse of Ψ*

Proof. Assume that $(S, *, \tilde{*})$ satisfies (1.8). Let (s', t') belong to $S \times S$. Put $s = t' \tilde{*} s'$ and $t = s' \tilde{*} t'$. By (1.8), we have $s * t = s'$ and $t * s = t'$, whence $\Psi(s, t) = (s', t')$. So Ψ is surjective. Conversely, assume $\Psi(s, t) = (s', t')$. Then the left-hand equality in (1.8) gives $s = t' * s'$ and $t = s' * t'$. So Ψ is injective. Moreover, the equalities show that the map $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is Ψ^{-1} . So (i) implies (ii).

Conversely, if Ψ is a bijection from $S \times S$ to itself, defining $s' \tilde{*} t'$ to be the unique t satisfying $s * t = s'$ and $t * s = t'$ for some s guarantees that $(s, t) \mapsto (s \tilde{*} t, t \tilde{*} s)$ is Ψ^{-1} . Then (1.8) is satisfied by definition, that is, (ii) implies (i). \square

Summarizing, we see that nondegenerate involutive set-theoretic solutions of the Yang–Baxter equation, involutive biracks, bijective RC-quasigroups, and RLC-quasigroups are entirely equivalent frameworks.

Convention 1.8. From now on, we write “solution of YBE” for “involutive non-degenerate set-theoretic solution of YBE”.

According to [16], a group and a monoid are associated with every solution of YBE, hence, equivalently, with every (bijective) RC-quasigroup.

Definition 1.9. The *structure group* (resp. *monoid*) associated with a solution (S, ρ) of YBE is the group (resp. *monoid*) defined by the presentation

$$(1.9) \quad \langle S \mid \{ab = a'b' \mid a, b, a', b' \in S \text{ satisfying } \rho(a, b) = (a', b')\} \rangle.$$

The *structure group* (resp. *monoid*) associated with an RC-quasigroup $(S, *)$ is the group (resp. *monoid*) defined by the presentation

$$(1.10) \quad \langle S \mid \{s(s * t) = t(t * s) \mid s \neq t \in S\} \rangle.$$

Such monoids and groups will be the main subject of investigation in this paper. The first observation is that, as can be expected, the monoids and groups associated with solutions of YBE and with bijective RC-quasigroups coincide.

Lemma 1.10. *If a solution (S, ρ) of YBE and a bijective RC-quasigroup $(S, *)$ are connected as in Proposition 1.5, then the structure monoids of (S, ρ) and $(S, *)$ coincide, and so do the corresponding groups.*

The result directly follows from the connection of Proposition 1.5, which shows that the relations of (1.9) and (1.10) coincide, up to some repetitions and adding trivial relations $ab = ab$ in (1.9).

Thus investigating structure monoids of solutions of YBE and of bijective RC-quasigroups are equivalent tasks. The goal of this paper is to show the advantages of the second approach.

2. RC-CALCULUS

In order to exploit the RC-law, we introduce sorts of polynomials involving the RC-operation and establish various algebraic relations that will be heavily used in the sequel. Most verifications are easy, but introducing convenient notation is important to obtain simple formulas and perform computations that, otherwise, would require tedious developments. It should be mentioned that some formulas admit counterparts in the world of braces [28, 29], which are equivalent to linear RC-systems, defined to be RC-systems equipped with a compatible abelian group operation (by [27, Prop. 6], the group G associated with a bijective RC-quasigroup $(S, *)$ is the brace $\mathbb{Z}^{(S)}$ with the Jacobson circle operation).

Everywhere in the sequel, $\tilde{*}$, $*$, and \cdot refer to binary operations.

Definition 2.1. For $n \geq 1$, we inductively define formal expressions $\Omega_n(x_1, \dots, x_n)$ and $\tilde{\Omega}_n(x_1, \dots, x_n)$ by $\Omega_1(x_1) = \tilde{\Omega}_1(x_1) = x_1$ and

$$(2.1) \quad \Omega_n(x_1, \dots, x_n) = \Omega_{n-1}(x_1, \dots, x_{n-1}) * \Omega_{n-1}(x_1, \dots, x_{n-2}, x_n),$$

$$(2.2) \quad \tilde{\Omega}_n(x_1, \dots, x_n) = \tilde{\Omega}_{n-1}(x_1, x_3, \dots, x_n) \tilde{*} \tilde{\Omega}_{n-1}(x_2, \dots, x_n).$$

The expression $\Omega_n(x_1, \dots, x_n)$ is a sort of n -variable monomial involving $*$. We find $\Omega_2(x_1, x_2) = x_1 * x_2$, then $\Omega_3(x_1, x_2, x_3) = (x_1 * x_2) * (x_1 * x_3)$, etc. Clearly, 2^{n-1} variables x_i occur in $\Omega_n(x_1, \dots, x_n)$, with brackets as in a balanced binary tree. In the language of braces, $\Omega_n(x_1, \dots, x_n)$ would correspond to $(x_1 + \dots + x_n) * x_n$.

If $(S, \tilde{*})$ is an algebraic system, $\Omega_n(s_1, \dots, s_n)$ is the evaluation of $\Omega_n(x_1, \dots, x_n)$ when x_i is given the value s_n . The next result is an iterated version of the RC-law.

Lemma 2.2. *Assume that $(S, *)$ is an RC-system. Then, for all s_1, \dots, s_n in S and π in \mathfrak{S}_{n-1} , we have $\Omega_n(s_{\pi(1)}, \dots, s_{\pi(n-1)}, s_n) = \Omega_n(s_1, \dots, s_n)$.*

It suffices to verify the result when π is a transposition of adjacent entries, and then the result follows from an obvious induction on $n \geq 3$, the case $n = 3$ precisely corresponding to the RC-law.

Of course, the counterpart of Lemma 2.2 involving $\tilde{\Omega}_n$ is valid when $\tilde{*}$ satisfies the LC-law (1.7). Further results appear when the monomials Ω_n are evaluated in an RC-quasigroup, that is, when left-translations are one-to-one.

Lemma 2.3. *Assume that $(S, *)$ is an RC-quasigroup and s_1, \dots, s_n lie in S .*

- (i) *The map $s \mapsto \Omega_{n+1}(s_1, \dots, s_n, s)$ is a bijection of S into itself.*

- (ii) There exist r_1, \dots, r_n in S satisfying $\Omega_i(r_1, \dots, r_i) = s_i$ for $1 \leq i \leq n$.
 (iii) Put $\tilde{s}_i = \Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_n, s_i)$ for $1 \leq i \leq n$. Then, for all i, j , the relations $s_i = s_j$ and $\tilde{s}_i = \tilde{s}_j$ are equivalent.

Proof. (i) Use induction on n . For $n = 1$, the result directly follows from the assumption. For $n \geq 2$, we have $\Omega_{n+1}(s_1, \dots, s_n, s) = t * \Omega_n(s_1, \dots, s_{n-1}, s)$ with $t = \Omega_n(s_1, \dots, s_{n-1})$. By induction hypothesis, $s \mapsto \Omega_n(s_1, \dots, s_{n-1}, s)$ is bijective. Composing with the left-translation by t yields a bijection.

(ii) Use induction on n . For $n = 1$, take $t_1 = s_1$. Assume $n \geq 2$. By induction hypothesis, there exist r_1, \dots, r_{n-1} satisfying $\Omega_i(r_1, \dots, r_i) = s_i$ for $1 \leq i \leq n-1$. Then, by definition of Ω_n and owing to $\Omega_{n-1}(r_1, \dots, r_{n-1}) = s_{n-1}$, we have $\Omega_n(r_1, \dots, r_{n-1}, x) = s_{n-1} * \Omega_{n-1}(r_1, \dots, r_{n-2}, x)$. As the left-translation by s_{n-1} is surjective, there exists s satisfying $s_{n-1} * s = s_n$. Then, by (i), there exists r_n satisfying $\Omega_{n-1}(r_1, \dots, r_{n-2}, r_n) = s$, whence $\Omega_n(r_1, \dots, r_n) = s_n$.

(iii) Again an induction on n . For $n = 1$ there is nothing to prove. For $n = 2$, we find $\tilde{s}_1 = s_2 * s_1$ and $\tilde{s}_2 = s_1 * s_1$, and $s_1 = s_2$ implies $\tilde{s}_1 = \tilde{s}_2$. Conversely, assume $s_1 * s_2 = s_2 * s_1$. Using the assumption twice and the RC-law, we obtain $(s_1 * s_2) * (s_2 * s_2) = (s_2 * s_1) * (s_2 * s_2) = (s_1 * s_2) * (s_1 * s_2) = (s_1 * s_2) * (s_2 * s_1)$. As left-translations are injective, we deduce $s_2 * s_2 = s_2 * s_1$, and $s_2 = s_1$. Assume now $n \geq 3$. Fix i, j , write \vec{s} for $s_1, \dots, \widehat{s}_i, \dots, \widehat{s}_j, \dots, s_n$ and put $t_k = \Omega_{n-1}(\vec{s}, s_k)$. Then, by (i) and by definition, we have $\tilde{s}_i = \Omega_n(\vec{s}, s_j, s_i) = \Omega_{n-1}(\vec{s}, s_j) * \Omega_{n-1}(\vec{s}, s_i) = t_j * t_i$, and, similarly, $\tilde{s}_j = t_i * t_j$. If $s_i = s_j$ holds, we have $t_i = t_j$, whence $\tilde{s}_i = \tilde{s}_j$. Conversely, assume $\tilde{s}_i = \tilde{s}_j$, that is, $t_j * t_i = t_i * t_j$. By the result for $n = 2$, we deduce $t_i = t_j$, that is, $\Omega_{n-1}(\vec{s}, s_i) = \Omega_{n-1}(\vec{s}, s_j)$, which is an equality of the form $r_1 * (\dots * (r_{n-2} * s_i) \dots) = r_1 * (\dots * (r_{n-2} * s_j) \dots)$. Repeatedly using the injectivity of left-translations, we deduce $s_i = s_j$. \square

Further results appear when two operations connected by (1.8) are involved. In terms of Ω_1 and Ω_2 , (1.8) says that $\tilde{s}_1 = \Omega_2(s_1, s_2)$ and $\tilde{s}_2 = \Omega_2(s_2, s_1)$ imply $s_1 = \tilde{\Omega}_2(\tilde{s}_1, \tilde{s}_2)$ and $s_2 = \tilde{\Omega}_2(\tilde{s}_2, \tilde{s}_1)$: two elements can be retrieved from their Ω_2 images using the monomial $\tilde{\Omega}_2$. Here is an n -variable version of this result.

Lemma 2.4. *Assume that $(S, *, \tilde{*})$ is an RLC-system and s_1, \dots, s_n belong to S . For $1 \leq i \leq n$, put $\tilde{s}_i = \Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_n, s_i)$. Then, for $1 \leq i \leq n$, and for every permutation π in \mathfrak{S}_n , we have*

$$(2.3) \quad \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) = \tilde{\Omega}_{n+1-i}(\tilde{s}_{\pi(i)}, \dots, \tilde{s}_{\pi(n)}).$$

Proof. For $n = 1$, (2.3) reduces to $s_{\pi(1)} = s_{\pi(1)}$. Fix $n \geq 2$ and use induction on i decreasing from n to 1. For $i = n$, (2.3) is $\Omega_n(s_{\pi(1)}, \dots, s_{\pi(i)}) = \tilde{\Omega}_1(\tilde{s}_{\pi(i)})$. By Lemma 2.2, the left term is $\Omega_n(s_1, \dots, \widehat{s}_i, \dots, s_{n-1}, s_{\pi(i)})$, hence $\tilde{s}_{\pi(i)}$, hence (2.3). Assume now $i < n$. Put $s = \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)})$, $s' = \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i-1)}, s_{\pi(i+1)})$, $t = \Omega_{i+1}(s_{\pi(1)}, \dots, s_{\pi(i)}, s_{\pi(i+1)})$, and $t' = \Omega_{i+1}(s_{\pi(1)}, \dots, s_{\pi(i-1)}, s_{\pi(i+1)}, s_{\pi(i)})$. Using the definition of Ω_{i+1} from Ω_i , we find $t = s * s'$ and $t' = s' * s$, whence $s = t' \tilde{*} t$ and $s' = t \tilde{*} t$ by the involutivity law. Now the induction hypothesis gives

$$t = \tilde{\Omega}_{n-i}(\tilde{s}_{\pi(i+1)}, \dots, \tilde{s}_{\pi(n)}), \quad t' = \tilde{\Omega}_{n-i}(\tilde{s}_{\pi(i)}, \tilde{s}_{\pi(i+2)}, \dots, \tilde{s}_{\pi(n)}).$$

Using the definition of Π_{n+1-i} from Π_{n-i} , we find $s = t' \tilde{*} t = \tilde{\Omega}_{n+1-i}(\tilde{s}_{\pi(i)}, \dots, \tilde{s}_{\pi(n)})$ (and $s' = t \tilde{*} t = \tilde{\Omega}_{n+1-i}(\tilde{s}_{\pi(i+1)}, \tilde{s}_{\pi(i)}, \tilde{s}_{\pi(i+2)}, \dots, \tilde{s}_{\pi(n)})$), which is (2.3). \square

We now introduce terms that involve, in addition to $*$ and $\tilde{*}$, a third operation \cdot that will be evaluated into an associative product.

Definition 2.5. For $n \geq 1$, we introduce the formal expressions

$$(2.4) \quad \Pi_n(x_1, \dots, x_n) = \Omega_1(x_1) \cdot \Omega_2(x_1, x_2) \cdot \dots \cdot \Omega_n(x_1, \dots, x_n)$$

$$(2.5) \quad \tilde{\Pi}_n(x_1, \dots, x_n) = \tilde{\Omega}_n(x_1, \dots, x_n) \cdot \tilde{\Omega}_{n-1}(x_2, \dots, x_n) \cdot \dots \cdot \tilde{\Omega}_1(x_n).$$

For $n \geq 2$, (2.4) implies $\Pi_n(x_1, \dots, x_n) = \Pi_{n-1}(x_1, \dots, x_{n-1}) \cdot \Omega_n(x_1, \dots, x_n)$. We shall consider below a monoid generated by S satisfying $s(s * t) = t(t * s)$, that is, $\Pi_2(s, t) = \Pi_2(t, s)$. Then we have the following iterated version.

Lemma 2.6. *Assume that $(S, *)$ is an RC-system and M is a monoid including S in which $\Pi_2(s, t) = \Pi_2(t, s)$ holds for all s, t in S . Then the evaluation of Π_n in M is a symmetric function on S^n .*

Proof. We use induction on n . For $n = 1$, there is nothing to prove. For $n = 2$, the result is the equality $s_1(s_1 * s_2) = s_2(s_2 * s_1)$, which is valid in M by assumption. Assume $n \geq 3$. As in Lemma 2.2, it is sufficient to consider transpositions $(i, i+1)$, that is, to compare $\Pi_n(s_1, \dots, s_n)$ and $\Pi_n(s_1, \dots, s_{i+1}, s_i, \dots, s_n)$. By definition, $\Pi_n(s_1, \dots, s_n)$ is the product of the values $\Omega_j(s_1, \dots, s_j)$ for j increasing from 1 to n , whereas $\Pi_n(s_1, \dots, s_{i+1}, s_i, \dots, s_n)$ is a similar product of $\Omega_j(s'_1, \dots, s'_j)$ with $s'_i = s_{i+1}$, $s'_{i+1} = s_i$, and $s'_k = s_k$ for $k \neq i, i+1$. For $j < i$, the entries s_i and s_{i+1} do not occur in $\Omega_j(s_1, \dots, s_j)$ and $\Omega_j(s'_1, \dots, s'_j)$, which are therefore equal. For $j > i+1$, the expressions $\Omega_j(s_1, \dots, s_j)$ and $\Omega_j(s'_1, \dots, s'_j)$ differ by the permutation of two non-final entries, so they are equal by Lemma 2.2. There remains to compare the central entries $t = \Omega_i(s_1, \dots, s_i) \cdot \Omega_{i+1}(s_1, \dots, s_{i+1})$ and $t' = \Omega_i(s'_1, \dots, s'_i) \cdot \Omega_{i+1}(s'_1, \dots, s'_{i+1})$. Put $r = \Omega_i(s_1, \dots, s_i)$ and $r' = \Omega_i(s_1, \dots, s_{i-1}, s_{i+1})$. By definition of s'_k , we have also $r = \Omega_i(s'_1, \dots, s'_{i-1}, s'_{i+1})$ and $r' = \Omega_i(s'_1, \dots, s'_i)$. Then, by definition of Ω_i and Ω_{i+1} , we have $t = r(r * r')$ and $t' = r'(r' * r)$, whence $t = t'$ in M . \square

Lemma 2.6 says in particular that, when we start with n elements s_1, \dots, s_n and construct in the Cayley graph of M the n -cube displayed in Figure 2, then the cube converges to a unique final vertex and all maximal paths represent $\Pi(s_1, \dots, s_n)$.

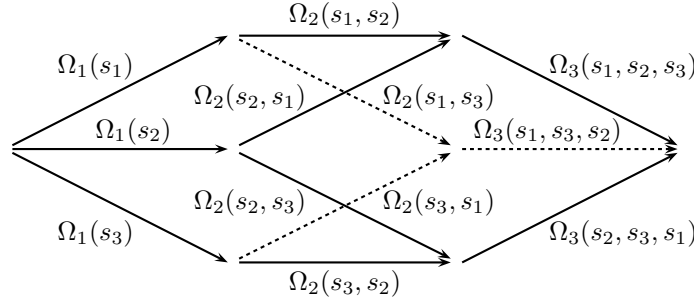


FIGURE 2. The monomials Ω_i occur at the i th level in an n -cube built from s_1, \dots, s_n using $*$ to form elementary squares (here $n = 3$).

Lemma 2.7. *Assume that $(S, *, \tilde{*})$ is an RLC-system and M is a monoid including S in which $\Pi(s, t) = \Pi(t, s)$ holds for all s, t in S . Then, for all s_1, \dots, s_n in S , the equality $\Pi_n(s_1, \dots, s_n) = \tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n)$ holds for $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$.*

Proof. Using (2.3) and the definitions of Π_n and $\tilde{\Pi}_n$, we obtain

$$\begin{aligned}\Pi_n(s_1, \dots, s_n) &= \Omega_1(s_1) \cdot \Omega_2(s_1, s_2) \cdot \dots \cdot \Omega_n(s_1, \dots, s_n) \\ &= \tilde{\Omega}_n(\tilde{s}_1, \dots, \tilde{s}_n) \cdot \tilde{\Omega}_{n-1}(\tilde{s}_2, \dots, \tilde{s}_n) \cdot \dots \cdot \tilde{\Omega}_1(\tilde{s}_n) = \tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n). \quad \square\end{aligned}$$

3. THE GARSIDE STRUCTURE

It was proved by F. Chouraqui [5] that the monoids associated with solutions of YBE (hence with bijective RC-quasigroups) are Garside monoids [9] and that, conversely, every Garside monoid with a certain type of presentation arises in this way—see also [19]. Here we show how to easily derive such results from the computations of Section 2.

Let us first recall some terminology about divisibility relations in monoids. If M is a (left)-cancellative monoid and f, g belong to M , we say that f *left-divides* g or, equivalently, that g is a *right-multiple* of f , denoted $f \preceq g$, if $fg' = g$ holds for some g' in M . If 1 is the only invertible element in M , the relation \preceq is a partial ordering on M . We say that h is a *least common right-multiple*, or *right-lcm*, of f and g if h is a least upper bound of f and g with respect to \preceq . Provided 1 is the only invertible element in M , the right-lcm is unique when it exists. If f and g admit a right-lcm, the *right-complement* $f \setminus g$ of f in g is the unique element g' such that fg' is the right-lcm of f and g . As mentioned in Example 1.4, \setminus obeys the RC-law (whenever defined). Of course, symmetric counterparts involve the right-divisibility relation, where f *right-divides* g if $g = g'f$ holds for some g' .

If M is a monoid, a *length function* on M is a map $\lambda : M \rightarrow \mathbb{N}$ such that $g \neq 1$ implies $\lambda(g) \geq 1$ and $\lambda(gh) = \lambda(g) + \lambda(h)$ always holds (we say *pseudolength* when $=$ is relaxed into \geq in the last formula). Note that the existence of a (pseudo)-length function on M implies that 1 is the only invertible element in M .

Our first (new) observation is that the connection between the RC-law and the so-called cube condition in Garside theory makes it extremely easy to establish the basic properties of the monoid associated with an RC-quasigroup.

Proposition 3.1. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then the monoid M admits a length function, it is left-cancellative, and any two elements of M admit a unique right-lcm and a unique left-gcd. Moreover, $(S, *)$ can be retrieved from M : the set S is the set of atoms of M and, for $s \neq t$, the value of $s * t$ is the right-complement $s \setminus t$ in M and the value of $s * s$ is the unique element of $S \setminus \{s \setminus t \mid t \neq s \in S\}$.*

Proof. The relations of (1.10) preserve the length, so the length of S -words induces a length function on M .

Next, the presentation (1.10) contains exactly one relation of the form $s\dots = t\dots$ for each pair of generators s, t in S . There exists for such presentations, which are called *right-complemented*, a general approach that enables one to easily establish properties of the associated monoid. Assume we consider a monoid generated by a set S and relations of the form $s\theta(s, t) = t\theta(t, s)$ where θ maps $S \times S$ to S . Then [10, Prop. 6.1 and 6.9] (or [12, Prop. II.4.16]) says that, when the “cube condition”

$$(3.1) \quad \theta(\theta(r, s), \theta(r, t)) = \theta(\theta(s, r), \theta(s, t))$$

holds for all r, s, t in S , the involved monoid is left-cancellative, any two of its elements admit a right-lcm, and the right-lcm of distinct elements s, t of S is $s(s * t)$ (and $t(t * s)$). In the current case of M , the map θ coincides with the operation $*$,

and the assumption that $(S, *)$ obeys the RC-law guarantees that (3.1) is satisfied. Hence M is left-cancellative and any two elements of M admit a right-lcm. Standard general arguments then show that any two elements also admit a left-gcd, that is, a greatest lower bound with respect to the left-divisibility relation.

Finally, as there is no relation involving a word of length one in (1.10), the elements of S are atoms, and every element not lying in $S \cup \{1\}$ is not an atom. So S is the atom set of M . Next, for distinct s, t in S , the right-lcm of s and t is $s(s * t)$, so, by definition, $s \setminus t$ is equal to $s * t$. Thus all nondiagonal values $s * t$ can be retrieved from M . Finally, all left-translations of $(S, *)$ are one-to-one, so $s * s$ must be the unique element of $S \setminus \{s * t \mid s, t \in S, s \neq t\}$, that is, of $S \setminus \{s \setminus t \mid t \neq s \in S\}$. \square

Corollary 3.2. *Assume that $(S, *)$ is a bijective RC-quasigroup and M, G are the associated structure monoid and group. Then M admits unique left- and right-lcms and left- and right-gcds, it is a Ore monoid, and G is a group of left- and right-fractions for M ; this group is torsion-free.*

Proof. Proposition 3.1 guarantees left-cancellativity and existence of right-lcms and left-gcds in M . Now, by Lemma 1.7, there exists a second operation $\tilde{*}$ on S such that $(S, *, \tilde{*})$ is an RLC-quasigroup. By construction, the presentation

$$(3.2) \quad \langle S \mid \{(s \tilde{*} t)t = (t \tilde{*} s)s \mid s \neq t \in S\} \rangle^+,$$

coincides with the one of (1.10). Proposition 3.1 applied to the opposed monoid M^{opp} and to the RC-quasigroup $(S, \tilde{*}^{\text{opp}})$ implies that M^{opp} is left-cancellative and admits right-lcms and left-gcds, hence M is right-cancellative and admits left-lcms and right-gcds. Hence M is in particular a Ore monoid (that is, a cancellative monoid where any two elements admit common left- and right-multiples). By a classical theorem of Ore [7], its enveloping group G , which admits as a group the presentation (1.10), is a group of left- and right-fractions for M . It is then known [11] that the group of fractions of a torsion-free monoid is torsion-free. \square

We can now use the RC-calculus of Section 2 to easily describe the right-lcms of atoms in terms of the “polynomials” Π_n , thus avoiding the developments of [5].

Lemma 3.3. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then elements s_1, \dots, s_n of S are pairwise distinct if and only if the element $\Pi_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n in M . In this case, if, in addition, $(S, *)$ is bijective, $\Pi_n(s_1, \dots, s_n)$ is also the left-lcm of the elements $\tilde{s}_1, \dots, \tilde{s}_n$ defined by $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$.*

Proof. Assume that s_1, \dots, s_n are pairwise distinct in S . Let Ω'_n and Π'_n be the counterparts of Ω_n and Π_n respectively where the right-complement operation \setminus replaces $*$. We first prove using induction on i the equality

$$(3.3) \quad \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)}) = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})$$

for every i and every permutation π in \mathfrak{S}_i . For $i = 1$, we have $\Omega_1(s_{\pi(1)}) = s_{\pi(1)} = \Omega'_1(s_{\pi(1)})$, and the result is straightforward. Assume $i \geq 2$. Put $s = \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)})$, $s' = \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}, s_{\pi(i-1)})$, $t = \Omega_i(s_{\pi(1)}, \dots, s_{\pi(i)})$, and $t' = \Omega_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)})$. By definition of Ω_i from Ω_{i-1} , we have $s = t * t'$ and $s' = t' * t$. By Lemma 2.3 applied to $(s_{\pi(1)}, \dots, s_{\pi(i)})$, the assumption $s_{\pi(i-1)} \neq s_{\pi(i)}$ implies $s \neq s'$, which implies $t * t' \neq t' * t$. By Proposition 3.1, the latter relation implies $t * t' = t \setminus t'$ and $t' * t = t' \setminus t$ in M . The induction

hypothesis implies $t = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})$ and $t' = \Omega'_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)})$, so we deduce $s = t \setminus t' = (\Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})) \setminus (\Omega'_{i-1}(s_{\pi(1)}, \dots, s_{\pi(i-2)}, s_{\pi(i)}))$, that is, $s = \Omega'_i(s_{\pi(1)}, \dots, s_{\pi(i)})$. Then (3.3) implies $\Pi_n(s_1, \dots, s_n) = \Pi'_n(s_1, \dots, s_n)$, meaning that $\Pi_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n since a trivial induction shows that $\Pi'_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n for every n .

For the other direction, let n' be the cardinal of $\{s_1, \dots, s_n\}$. The result above implies that, if I is a cardinal n' subset of S , then the right-lcm Δ_I of I has length n' in M . So, if $n' < n$ holds, the right-lcm of $\{s_1, \dots, s_n\}$ is an element of M that has length n' , and it cannot be $\Pi_n(s_1, \dots, s_n)$ which, by definition, has length n .

Finally, assume that $(S, *)$ is bijective and s_1, \dots, s_n are pairwise distinct. Let $\tilde{*}$ be the second operation provided by Lemma 1.7. Then $(S, *, \tilde{*})$ is an RLC-quasigroup. By Lemma 2.3, $\tilde{s}_1, \dots, \tilde{s}_n$ are pairwise distinct. Then $(S, \tilde{*})$ is an LC-quasigroup, so the counterpart of the above results implies that $\tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n)$ is a left-lcm of $\tilde{s}_1, \dots, \tilde{s}_n$ in M . Now, by Lemma 2.7, $\tilde{\Pi}_n(\tilde{s}_1, \dots, \tilde{s}_n)$ is equal to $\Pi_n(s_1, \dots, s_n)$. \square

A *Garside family* [13] in a monoid M is a generating family Σ such that every element g of M admits a (unique) Σ -normal decomposition, meaning a sequence (s_1, \dots, s_p) such that $g = s_1 \cdots s_p$ holds and s_i is the greatest left-divisor of $s_i \cdots s_p$ lying in Σ for every i .

Proposition 3.4. *Assume that $(S, *)$ is a bijective RC-quasigroup and M, G are the associated monoid and group. Then the right-lcm Δ_I of a cardinal n subset I of S belongs to S^n , it is the left-lcm of (another) cardinal n subset of S , the map $I \mapsto \Delta_I$ is injective, and its image is the smallest Garside family of M that contains 1.*

Proof. By Proposition 3.1, M admits a length function, it is left-cancellative, and that any two elements of M admit a right-lcm. Hence, by [13, Prop. 3.25] (or [12, Prop. IV.2.46]), M admits a smallest Garside family Σ , namely the closure of the atoms, that is, of S , under the right-lcm and right-complement operations. We claim that Σ is the closure Σ' of S under the sole right-lcm operation.

By definition, Σ' is included in Σ , and the point is to prove that Σ' is closed under the right-complement operation. This follows from the formula

$$(3.4) \quad f \setminus \text{lcm}(g_1, \dots, g_n) = \text{lcm}(f \setminus g_1, \dots, f \setminus g_n),$$

which is valid in every monoid that admits unique right-lcms as shows an easy induction on n . So assume that g belongs to Σ' , that is, g is a right-lcm of elements t_1, \dots, t_n of S . If f lies in S , then, for every i , the element $f \setminus t_i$ belongs to $S \cup \{1\}$ since it is either $f * t_i$, if f and t_i are distinct, or 1, if f and t_i coincide. Then (3.4) shows that $f \setminus g$ belongs to Σ' for every f in S . Using induction on the length of f , we deduce a similar result for every f in M from the formula $(f_1 f_2) \setminus g = f_2 \setminus (f_1 \setminus g)$. So Σ' is closed under \setminus and it coincides with Σ .

For I a finite subset of S , write Δ_I for the right-lcm of I . Lemma 3.3 shows that Δ_I has length $\#I$. Now, assume that I, J are finite subsets of S and $\Delta_I = \Delta_J$ holds. As every element of $I \cup J$ left-divides Δ_I , we must have $\Delta_{I \cup J} = \Delta_I = \Delta_J$. This implies $\#(I \cup J) = \#I = \#J$, whence $I = I \cup J = J$. So the map $I \mapsto \Delta_I$ is a bijection of $\mathfrak{P}_{fin}(S)$ to Σ .

Finally, if s_1, \dots, s_n are pairwise distinct elements of S , then $\Pi_n(s_1, \dots, s_n)$ is the right-lcm of s_1, \dots, s_n and, by Lemma 3.3, the latter is also the left-lcm of the elements $\tilde{s}_1, \dots, \tilde{s}_n$ defined by $\tilde{s}_i = \Omega_n(s_1, \dots, \hat{s}_i, \dots, s_n, s_i)$. \square

We turn to Garside monoids [9]. A pair (M, Δ) is a *Garside monoid* if M is a cancellative monoid, it admits a weak length function, every two elements admit left- and right-lcms and gcds, and Δ is a Garside element in M , meaning that the left- and right-divisors of Δ coincide, generate M , and are finite in number. We often say that a monoid M is a Garside monoid if there exists Δ in M such that (M, Δ) satisfies the above conditions.

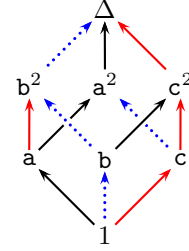
Proposition 3.5. *Assume that $(S, *)$ is a bijective RC-quasigroup of cardinal n and M is the associated monoid. Then the right-lcm Δ of S is a Garside element in M , it admits 2^n (left- or right-) divisors, and (M, Δ) is a Garside monoid.*

Proof. As above, write Δ_I for the right-lcm of I for $I \subseteq S$, and write Δ for Δ_S . By Proposition 3.4, the family Σ of all elements Δ_I is the smallest Garside family containing 1 in M , and it has 2^n elements. By definition, Δ_I left-divides Δ_S , that is, every element of Σ left-divides Δ , and, moreover, Δ lies in Σ . This means that the Garside family Σ is what is called right-bounded by Δ [12, Def. VI.1.1], and Δ is a right-Garside element in M . Moreover, by Corollary 3.2, M is also right-cancellative, and Σ is a finite subset of M that generates M and is closed under the right-complement operation. By [9, Prop. 2.1], Δ is a Garside element in M , and (M, Δ) is a Garside monoid. \square

Example 3.6. Let $S = \{a, b, c\}$, and let $*$ be determined by $x * y = f(y)$ where f is the cycle $a \mapsto b \mapsto c \mapsto a$. Then, as seen in Example 1.4, $(S, *)$ is a bijective RC-quasigroup, and it is eligible for the above results. The associated monoid admits the presentation

$$\langle a, b, c \mid ac = b^2, a^2 = cb, ba = c^2 \rangle^+.$$

The right-lcm Δ of S is then a^3 , which is also b^3 and c^3 , and the lattice of the 8 divisors of Δ is shown on the right.



We conclude the section with a result in the other direction. If (S, ρ) is a solution of the YBE or, equivalently, if $(S, *)$ is a finite bijective RC-quasigroup, then the associated monoid is a Garside monoid and, moreover, its definition implies that the latter admits a presentation of a certain form. We see now is that, conversely, every Garside monoid with the above properties is associated with a (bijective) RC-quasigroup. Once again, a YBE version appears in [5] and the point here is to show that using the RC-law provides alternative and hopefully more simple arguments.

Proposition 3.7. *Assume that M is a monoid with atom set S of cardinal n . Then the following are equivalent:*

- (i) *There exists an operation $*$ such that $(S, *)$ is a bijective RC-quasigroup and M is associated with $(S, *)$ —or, equivalently, there exists ρ such that (S, ρ) is a solution of YBE and M is associated with (S, ρ) ;*
- (ii) *The monoid M is a Garside monoid admitting a presentation in terms of S that consists of one relation $s\theta(s, t) = t\theta(t, s)$ for $s \neq t$ in S with $\theta : S \times S \rightarrow S$ such that $t \mapsto \theta(s, t)$ is injective for every s .*
- (iii) *The monoid M is a Garside monoid admitting a presentation in terms of S consisting of $\binom{n}{2}$ relations $u = v$ with u, v of length two such that every length two S -word appears in at most one relation.*

It follows from Definition 1.9 and Proposition 3.5 that (i) implies (ii); on the other hand, a presentation satisfying the conditions of (ii) necessarily satisfies those of (iii) since a length two S -word ss' may appear in a relation $s... = t...$ only if $s' = \theta(s, t)$ holds, which happens for at most one t . So we are left with proving that (iii) implies (ii) and that (ii) implies (i).

Proof of (iii) \Rightarrow (ii) in Proposition 3.7. Let R be the considered list of relations. Assume that s, t are distinct elements of S and R contains at least two relations $s... = t...$, say $st' = ts'$ and $st'' = ts''$ with $(s', t') \neq (s'', t'')$. As M is cancellative, we have $st' \neq st''$, so st' and st'' are two common right-multiples of s and t of length 2: this contradicts the existence of a right-lcm for s and t , as the latter can have neither length 1 nor length 2. Hence R contains at most one relation $s... = t...$ for $s \neq t$. On the other hand, R contains no relation $s... = s...$ since M is left-cancellative and $st = st'$ would imply $t = t'$. As there are $\binom{n}{2}$ pairs of distinct elements of S , we deduce that R contains exactly one relation $s... = t...$ for $s \neq t$ in S . We can then write the latter relation as $s\theta(s, t) = t\theta(t, s)$ for some map θ from S^2 to S . The assumption that no word appears in two relations then implies that every map $t \mapsto \theta(s, t)$ is injective. \square

We recall that, if M is a cancellative monoid in which any two elements admit a unique right-lcm, then, for f, g in M , the right-complement of f in g is the element $f \setminus g$ such that $f(f \setminus g)$ is the right-lcm of f and g . Under symmetric assumptions, the *left-complement* f/g is the element such that $(f/g)g$ is the left-lcm of f and g . The operation \setminus obeys the RC-law, whereas $/$ obeys the LC-law.

Proof of (ii) \Rightarrow (i) in Proposition 3.7. By assumption, $s\theta(s, t)$ is the right-lcm of s and t (which exists since M is a Garside monoid) for $s \neq t$ in S , so $s \setminus t = \theta(s, t)$ holds. We define a binary operation $*$ on S . First, we put $s * t = s \setminus t$ for $s \neq t$. As $t \neq t'$ implies $\theta(s, t) \neq \theta(s, t')$, the map $x \mapsto s * x$ is injective on $S \setminus \{s\}$, so the complement of $\{s * x \mid x \neq s\}$ in S consists of a unique element, which we define to be $s * s$. We thus obtain an operation $*$ whose left-translations are one-to-one.

Next, we know that (ii) implies (iii). Now, in (iii), the left and the right sides play symmetric roles. Hence the symmetric counterpart of (ii) is true and, by (the counterpart of) the above argument, we obtain a binary operation $\tilde{*}$ on S connected with the left-complement operation $/$ and such that the right-translations $\tilde{*}$ are one-to-one. We claim that $*$ and $\tilde{*}$ satisfy (1.8). First, assume $s \neq t$. Then $s(s * t) = t(t * s)$ lies in R (the considered set of relations), implying $s * t \neq t * s$. Next, $s(s * t)$ is the right-lcm of s and t , and, as $s * t$ and $t * s$ are distinct, $s(s * t)$ is the left-lcm of $s * t$ and $t * s$, which implies $(s * t) \tilde{*} (t * s) = t$. Now, put $s' = s * s$ and $r = s' \tilde{*} s'$. For $t \neq s$, we have $s * t \neq s'$, whence $r = s' / (s \setminus t)$. Then $r(s \setminus t) = ((s \setminus t) / s') s'$ is a relation of R , which implies $(s \setminus t) / s' \neq s$ since R contains no relation $ss' = \dots$. Since $(s \setminus t) / s' \neq s$ holds for every t distinct of s , we deduce $s' \tilde{*} s' = s$ since $s' \tilde{*} s'$ is the only element of S that is not of the form $(s \setminus t) \tilde{*} s'$ with $t \neq s$. Hence $(s * s) \tilde{*} (s * s) = s$ holds, and the first involutivity law is satisfied in $(S, *, \tilde{*})$. By a symmetric argument, the second involutivity law holds as well.

Finally, we claim that $(S, *)$ satisfies the RC-law. Let r, s, t lie in S . Assume first that r, s, t are pairwise distinct. Then we have $r * s \neq r * t$ and $s * r \neq s * t$, whence $(r * s) * (r * t) = (r \setminus s) \setminus (r \setminus t) = (s \setminus r) \setminus (s \setminus t) = (s * r) * (s * t)$, since the right-complement operation \setminus satisfies the RC-law. Next, for $r = s$, the RC-law tautologically holds for r, s, t . So there only remain the cases when $r \neq s$ and t is

either r or s , that is, we have to establish $(r * s) * (r * s) = (s * r) * (s * s)$ and $(s * r) * (s * r) = (r * s) * (r * r)$, that is, owing to $r \neq s$,

$$(3.5) \quad (r \setminus s) * (r \setminus s) = (s \setminus r) \setminus (s * s) \text{ and } (s \setminus r) * (s \setminus r) = (r \setminus s) \setminus (r * r).$$

Assume $z \neq r, s$ and put $z' = (r \setminus s) \setminus (r \setminus z)$, which is also $z' = (s \setminus r) \setminus (s \setminus z)$ since \setminus satisfies the RC-law. Then we have $r \setminus z \neq r \setminus s$, whence $z' \neq (r \setminus s) * (r \setminus s)$. Also, we have $s \setminus z \neq s * s$, whence $z' \neq (s \setminus r) \setminus (s * s)$. Arguing similarly with r and s exchanged, we find $z' \neq (s \setminus r) * (s \setminus r)$ and $z' \neq (r \setminus s) \setminus (r * r)$. So, z' is distinct from the four expressions occurring in (3.5) and, therefore, the only possible values for the latter are the two elements of S that are not of the form $(r \setminus s) \setminus (r \setminus z)$ with $z \neq r, s$. As left-translations of $*$ are injective, we must have $(r \setminus s) * (r \setminus s) \neq (r \setminus s) \setminus (r * r)$ and $(s \setminus r) \setminus (s * s) \neq (s \setminus r) * (s \setminus r)$. So, in order to establish (3.5), it suffices to show that $(r \setminus s) * (r \setminus s) = (s \setminus r) * (s \setminus r)$ is impossible. Now $r \neq s$ implies $r * s \neq s * s$, so it is enough to prove that $x \neq y$ implies $x * x \neq y * y$: this follows from the involutivity relation $(x * x) * (x * x) = x$ established above.

So $(S, *)$ is an RC-quasigroup. By [27, Theorem 2], it is necessarily bijective since S is finite—alternatively, one can check that $(S, *, *)$ is an RLC-quasigroup and $(S, *)$ is bijective by Lemma 1.7. By construction, M admits the presentation (S, R) , so it is (isomorphic to) the monoid associated with $(S, *)$. \square

Remark 3.8. The injectivity condition for left-translations associated with θ is necessary in Proposition 3.7(ii): the dual braid monoid $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \mid \mathbf{ab} = \mathbf{bc} = \mathbf{ca} \rangle^+$ is a Garside monoid that admits a presentation of the considered type but it is not associated with an RC-quasigroup since (for instance) the right-lcm of the atoms has 5 divisors. Now, in this case, we have $\theta(\mathbf{a}, \mathbf{b}) = \theta(\mathbf{a}, \mathbf{c}) = \mathbf{b}$.

4. THE I -STRUCTURE

It has been known since [20] and [24] that the monoids associated with solutions of YBE admit a nice geometric characterization as those monoids that admit an I -structure, meaning that their Cayley graph is a twisted copy of that of a free abelian monoid. These results can be easily established using the framework of RC-quasigroups and the computational formulas of Section 2. In particular, we shall see that the I -structure can be explicitly determined using the polynomials Π_n .

In view of the final results in Section 5, it is convenient to start with a slightly extended definition in which the reference monoid need not be free Abelian.

Definition 4.1. Assume that M_\bullet and M are monoids generated by a set S . A *right- I -structure of shape (M_\bullet, S)* for M is a bijective map $\nu : M_\bullet \rightarrow M$ satisfying $\nu(1) = 1$, $\nu(s) = s$ for s in S and, for every a in M_\bullet ,

$$(4.1) \quad \{\nu(as) \mid s \in S\} = \{\nu(a)s \mid s \in S\}.$$

When the reference monoid M_\bullet is the S -power of a monoid, we skip S and just say “right- I -structure of shape M_\bullet ”; if M_\bullet is a free Abelian monoid, we also skip M_\bullet and—as is usual—say “right- I -structure”. A monoid is said to be *of right- I -type* [20, 24] if it admits a right I -structure.

The existence of a right- I -structure of shape (M_\bullet, S) on a monoid M provides a bijection from the Cayley graph of M_\bullet relative to S onto that of M that preserves the path length but changes labels. Note that (4.1) is equivalent to the existence, for every a in M_\bullet , of a permutation $\psi(a)$ of S satisfying, for every s in S ,

$$(4.2) \quad \nu(as) = \nu(a) \cdot \psi(a)(s).$$

We shall use ψ with this meaning everywhere in the sequel.

If M_\bullet is a free Abelian monoid based on S and, more generally, if every permutation of S induces an automorphism of M_\bullet , then the condition $\nu(s) = s$ for s in S , which amounts to $\psi(1)$ being the identity of S , can be ensured by precomposing ν with the automorphism induced by $\psi(1)^{-1}$ and, therefore, it could be removed from the definition without changing the range of the latter.

Hereafter we denote by $\mathbb{N}^{(S)}$ the free Abelian monoid based on a (finite or infinite) set S , identified with the set of all finite support S -indexed sequences of elements of \mathbb{N} (we use \mathbb{N}^S when S is finite); an element s of S is identified with the sequence whose only non-zero entry is the s -entry, which is 1.

We first establish the following explicit “RC-version” of the result of [20, 24]:

Proposition 4.2. *Assume that $(S, *)$ is an RC-quasigroup and M is the associated monoid. Then the map ν defined from $*$ by $\nu(s_1 \cdots s_n) = \Pi_n(s_1, \dots, s_n)$ is a right I -structure on M .*

Proof. We first define a map ν^* from the free monoid S^* based on S to M by $\nu^*(\varepsilon) = 1$ and $\nu^*(s_1 | \cdots | s_n) = \Pi_n(s_1, \dots, s_n)$ for $n \geq 1$, where $s_1 | \cdots | s_n$ is the length n word with letters s_1, \dots, s_n . By Lemma 2.6, $\nu^*(s_1 | \cdots | s_n)$ does not depend on the order of the entries, so ν^* induces a well-defined map ν from the free Abelian monoid $\mathbb{N}^{(S)}$ to M . We claim that the latter provides the expected right- I -structure on M . First, the equalities $\nu(1) = 1$ and $\nu(s) = s$ for s in S are obvious. Next, let a belong to $\mathbb{N}^{(S)}$, say $a = s_1 \cdots s_n$. Then the definition of ν gives $\nu(as) = \Pi_{n+1}(s_1, \dots, s_n, s)$, whence $\nu(as) = \Pi_n(s_1, \dots, s_n) \cdot \Omega_{n+1}(s_1, \dots, s_n, s)$. By Lemma 2.3(i), the map $s \mapsto \nu(as)$ is a bijection of S into itself, hence (4.1) holds.

It remains to show that ν is a bijection from $\mathbb{N}^{(S)}$ to M . Let g belong to M , say $g = s_1 \cdots s_n$ with s_1, \dots, s_n in S . By Lemma 2.3(ii), there exist r_1, \dots, r_n in S satisfying $\Omega_i(r_1, \dots, r_i) = (s_1, \dots, s_i)$ for $1 \leq i \leq n$, whence $\Pi_n(r_1, \dots, r_n) = s_1 \cdots s_n = g$. By definition, this means that $\nu(r_1 \cdots r_n) = g$ holds, and ν is surjective.

Finally, assume that a, a' belong to $\mathbb{N}^{(S)}$ and $\nu(a) = \nu(a')$ holds. As the elements of M have a well-defined length, the length of a and a' must be the same. Write $a = r_1 \cdots r_n$, $a' = r'_1 \cdots r'_n$ with r_1, \dots, r'_n in S . Define $s_i = \Omega_i(r_1, \dots, r_i)$ and $s'_i = \Omega_i(r'_1, \dots, r'_i)$. By definition, $\nu(a)$ is the class of $s_1 | \cdots | s_n$ in M , and $\nu(a')$ is the class of $s'_1 | \cdots | s'_n$. The assumption $\nu(a) = \nu(a')$ means that these words are connected by a finite sequence of defining relations of M . By Lemma 2.3, the map $(x_1, \dots, x_n) \mapsto (\Omega_1(x_1), \dots, \Omega_n(x_1, \dots, x_n))$ of $S^{[n]}$ to itself is surjective, so we can assume without loss of generality that $s_1 | \cdots | s_n$ and $s'_1 | \cdots | s'_n$ are connected by one relation exactly, that is, there exist i satisfying $s_{i+1} = s_i * s'_i$, $s'_{i+1} = s'_i * s_i$ and $s'_k = s_k$ for $k \neq i, i+1$. The relations $s'_k = s_k$ inductively imply $r'_k = r_k$ for $k < i$. Next, writing \vec{r} for r_1, \dots, r_{i-1} , we have $s_i = \Omega_i(\vec{r}, r_i)$ and $s'_i = \Omega_i(\vec{r}, r'_i)$. Then, we find

$$\Omega_i(\vec{r}, r_i) * \Omega_i(\vec{r}, r_{i+1}) = \Omega_{i+1}(\vec{r}, r_i, r_{i+1}) = s_{i+1} = s_i * s'_i = \Omega_i(\vec{r}, r_i) * \Omega_i(\vec{r}, r'_i).$$

As the left-translation by $\Omega_i(\vec{r}, r_i)$ is injective, we deduce $\Omega_i(\vec{r}, r_{i+1}) = \Omega_i(\vec{r}, r'_i)$, whence $r_{i+1} = r'_i$ by Lemma 2.3(i). A symmetric argument gives $r'_{i+1} = r_i$. Finally, for $k > i+1$, the relations $s'_k = s_k$ inductively imply $r'_k = r_k$. Indeed, we have

$$\Omega_k(\vec{r}, r_i, r'_i, r_{i+2}, \dots, r_k) = s_k = s'_k = \Omega_k(\vec{r}, r'_i, r_i, r_{i+2}, \dots, r'_k),$$

and, by Lemma 2.2, switching the non-final entries r_i and r'_i in Ω_k changes nothing, so $r'_k = r_k$ follows by Lemma 2.3. So the words $r_1 | \cdots | r_n$ and $r'_1 | \cdots | r'_n$ are obtained

by switching two (adjacent) entries, hence they represent the same element in $\mathbb{N}^{(S)}$. Hence ν is injective, and it provides the expected right- I -structure on M . \square

Note that Proposition 4.2 does not require the set S to be finite.

In the other direction, we prove that every finitely generated monoid of I -type is associated with an RC-quasigroup, an explicit version of the YBE results of [20, 24]:

Proposition 4.3. *If M is a finitely generated monoid of right- I -type, there exists a unique finite RC-quasigroup $(S, *)$ such that M is the structure monoid of $(S, *)$: the set S is the atom set of M and $*$ is determined by $s * t = s \setminus t$ for $s \neq t$ and $\{s * s\} = S \setminus \{s \setminus t \mid t \neq s\}$. Moreover, the right- I -structure on M is unique: it is defined from the operation $*$ by $\nu(s_1 \cdots s_n) = \Pi_n(s_1, \dots, s_n)$.*

Once again our proof relies on RC-calculus. One of the benefits is to obtain an argument that, although complete, in particular for establishing (4.7) below, is shorter than that of [25, Chapter 8]. Another benefit is that Lemma 4.4 extends to a nonfree Abelian monoid, which will be useful in Section 5.

Lemma 4.4. *Assume that M is a left-cancellative monoid and ν is a right- I -structure of shape (M_\bullet, S) on M , where M_\bullet is Abelian and satisfies*

$$(4.3) \quad \forall s, t, s', t' \in S ((s \neq t \text{ and } st' = ts') \Rightarrow (s' = s \text{ and } t' = t)).$$

*Put $s * t = \psi(s)(t)$ for s, t in S . Then $(S, *)$ is an RC-quasigroup.*

Proof. We claim that, for all s, t, s', t' in S with $s \neq t$, the only equality $st' = ts'$ holding in M is $s(st) = t(ts)$. Indeed, by assumption, M_\bullet is Abelian and, in M , using (4.2), we obtain $s(st) = s\psi(s)(t) = \nu(st) = \nu(ts) = t\psi(t)(s) = t(ts)$. On the other hand, assume $st' = ts'$ in M . Let $t'_\bullet = \psi(s)^{-1}(t')$ and $s'_\bullet = \psi(t)^{-1}(s')$. Always using (4.2), we find $\nu(st'_\bullet) = st' = ts' = \nu(ts'_\bullet)$ in M , whence $st'_\bullet = ts'_\bullet$ in M_\bullet since ν is bijective. The assumption on M_\bullet implies $s'_\bullet = s$ and $t'_\bullet = t$, whence $s' = \psi(t)(s) = t * s$ and $t' = \psi(s)(t) = s * t$. This establishes the claim.

Now, let a belong to M_\bullet and s, t belong to S . Using (4.2), we find

$$\nu(ast) = \nu(as) \cdot \psi(as)(t) = \nu(a) \cdot \psi(a)(s) \cdot \psi(as)(t),$$

and, similarly, $\nu(ats) = \nu(a) \cdot \psi(a)(t) \cdot \psi(at)(s)$. By assumption, M_\bullet is Abelian, so we have $ast = ats$, whence $\nu(ast) = \nu(ats)$ and, merging the above expressions and left-cancelling $\nu(a)$, which is legal as M is left-cancellative, we find

$$(4.4) \quad \psi(a)(s) \cdot \psi(as)(t) = \psi(a)(t) \cdot \psi(at)(s).$$

Assume first $s \neq t$. The elements $\psi(a)(s)$, $\psi(as)(t)$, $\psi(a)(t)$, and $\psi(at)(s)$ lie in S , so, by the claim above, (4.4) implies

$$(4.5) \quad \psi(as)(t) = \psi(a)(s) * \psi(a)(t) \quad \text{and} \quad \psi(at)(s) = \psi(a)(t) * \psi(a)(s).$$

When t ranges over $S \setminus \{s\}$, the element $\psi(a)(t)$ ranges over $S \setminus \{\psi(a)(s)\}$, and $\psi(a)(s) * \psi(a)(t)$ ranges over $S \setminus \{\psi(a)(s) * \psi(a)(s)\}$. As $\psi(as)$ is a bijection of S , the only possibility is therefore $\psi(as)(s) = \psi(a)(s) * \psi(a)(s)$. Hence (4.5) is valid in S for all a in M_\bullet and s, t in S .

Now, let r lie in S . Making $a = r$ in (4.5) and applying the definition of $*$ gives $\psi(rs)(t) = (r * s) * (r * t)$ and, similarly, $\psi(sr)(t) = (s * r) * (s * t)$. Now, in M_\bullet , we have $rs = sr$, whence $\psi(rs)(t) = \psi(sr)(t)$, and this gives $(r * s) * (r * t) = (s * r) * (s * t)$, the RC-law. So $(S, *)$ is an RC-system. Moreover, by definition, $\psi(s)$ belongs to \mathfrak{S}_S , so the left-translations of $*$ are one-to-one, and $(S, *)$ is an RC-quasigroup. \square

Lemma 4.5. *Assume that M is a left-cancellative monoid and ν is a right- I -structure of shape (M_\bullet, S) on M , where M_\bullet is Abelian and satisfies (4.3). Then, for every $p \geq 1$ and for all s_1, \dots, s_p in S , we have*

$$(4.6) \quad \psi(s_1 \cdots s_{p-1})(s_p) = \Omega_p(s_1, \dots, s_p) \quad \text{and} \quad \nu(s_1 \cdots s_p) = \Pi_p(s_1, \dots, s_p),$$

where Ω_p and Π_p are associated with $*$ as in Section 2 and values are taken in M . Moreover, for all a, b in $\mathbb{N}^{(S)}$, we have

$$(4.7) \quad \nu(ab) = \nu(a)\nu(\psi(a)[b]) \quad \text{and} \quad \psi(ab) = \psi(\psi(a)[b]) \circ \psi(a)$$

where $\psi(a)[b]$ is the result of applying $\psi(a)$ to b componentwise.

Proof. We begin with the left equality in (4.6), which is proved using induction on p . For $p = 1$, we have $\psi(1)(s_1) = s_1 = \Omega_1(s_1)$ and, for $p = 2$, we have $\psi(s_1)(s_2) = s_1 * s_2 = \Omega_2(s_1, s_2)$. For $p \geq 3$, using (4.5), the induction hypothesis, and the inductive definition of the monomials Ω_p , we find

$$\begin{aligned} \psi(s_1 \cdots s_{p-1})(s_p) &= \psi(s_1 \cdots s_{p-2})(s_{p-1}) * \psi(s_1 \cdots s_{p-2})(s_p) \\ &= \Omega_{p-1}(s_1, \dots, s_{p-1}) * \Omega_{p-1}(s_1, \dots, s_{p-2}, s_p) = \Omega_p(s_1, \dots, s_p). \end{aligned}$$

The right equality in (4.6) then follows using a similar induction on p . For $p = 1$, we have $\nu(s_1) = s_1 = \Pi_1(s_1)$. For $p \geq 2$, using (4.2), the left equality in (4.6), and the inductive definition of Π_p , we find

$$\begin{aligned} \nu(s_1 \cdots s_p) &= \nu(s_1 \cdots s_{p-1}) \cdot \psi(s_1 \cdots s_{p-1})(s_p) \\ &= \Pi_{p-1}(s_1, \dots, s_{p-1}) \cdot \Omega_p(s_1, \dots, s_p) = \Pi_p(s_1, \dots, s_p). \end{aligned}$$

The definition of Ω_n implies, for $p, q \geq 1$, the formal equality

$$\Omega_{p+q}(\vec{x}, y_1, \dots, y_q) = \Omega_q(\Omega_{p+1}(\vec{x}, y_1), \dots, \Omega_{p+1}(\vec{x}, y_q)),$$

where \vec{x} stands for x_1, \dots, x_p ; this is a formal identity, not using the RC-law or any specific relation; for instance, it says that $\Omega_3(x, y_1, y_2)$, that is, $(x * y_1) * (x * y_2)$, is also $\Omega_2(\Omega_2(x, y_1), \Omega_2(x, y_2))$. With the same convention, one deduces

$$(4.8) \quad \Pi_{p+q}(\vec{x}, y_1, \dots, y_q) = \Pi_p(\vec{x}) \cdot \Pi_q(\Omega_{p+1}(\vec{x}, y_1), \dots, \Omega_{p+1}(\vec{x}, y_q)).$$

Now, assume that a, b lie in $\mathbb{N}^{(S)}$. Write $a = s_1 \cdots s_p$ and $b = t_1 \cdots t_q$ with s_1, \dots, t_q in S . The right equality in (4.6) gives $\nu(ab) = \Pi_{p+q}(s_1, \dots, s_p, t_1, \dots, t_q)$. On the other hand, we have $\nu(a) = \Pi_p(s_1, \dots, s_p)$ and the left equality in (4.6) implies $\psi(a)(t) = \Omega_{p+1}(s_1, \dots, s_p, t)$ for every t , whence in particular

$$\nu(\psi(a)(t)) = \Pi_q(\Omega_{p+1}(s_1, \dots, s_p, t_1), \dots, \Omega_{p+1}(s_1, \dots, s_p, t_q)).$$

Merging with (4.8), we obtain the left formula in (4.7).

Finally, assume $s \in S$. On the one hand, (4.2) gives $\nu(abs) = \nu(ab)\psi(ab)(s)$. On the other hand, the left formula in (4.7) gives

$$\begin{aligned} \nu(abs) &= \nu(a) \cdot \nu(\psi(a)[bs]) = \nu(a) \cdot \nu(\psi(a)[b] \cdot \psi(a)(s)) \\ &= \nu(a) \cdot \nu(\psi(a)[b]) \cdot \psi(\psi(a)[b])(\psi(a)(s)) = \nu(ab) \cdot \psi(\psi(a)[b])(\psi(a)(s)). \end{aligned}$$

Merging the two expressions and using the assumption that M is left-cancellative, we deduce $\psi(ab)(s) = \psi(\psi(a)[b])(\psi(a)(s))$, which is the right equality in (4.7). \square

We now connect left-divisibility with the I -structure, in the case of a right- I -structure of shape $(\mathbb{N}^{(S)}, S)$, that is, a genuine right- I -structure.

Lemma 4.6. *Assume that ν is a right- I -structure based on S in a monoid M .*

- (i) *There exists a length function on M and S is the atom set in M .*
- (ii) *The map ν is compatible with left-division in the sense that, for all a, b in $\mathbb{N}^{(S)}$, we have $a \preceq b$ in $\mathbb{N}^{(S)}$ if and only if $\nu(a) \preceq \nu(b)$ holds in M .*
- (iii) *The monoid M admits right-lcms.*

Proof. (i) Defining $\lambda(g)$ to be the length of $\nu^{-1}(g)$ provides a function from M to \mathbb{N} that satisfies $\lambda(1) = 0$, $\lambda(gh) = \lambda(g) + \lambda(h)$, and $\lambda(s) = 1$ for every s in S . It follows that M contains no nontrivial invertible element, and that S is the atom set of M .

(ii) Assume $a \preceq b$ in $\mathbb{N}^{(S)}$. For an induction on length, we may assume $b = as$ with s in S . Now, by (4.2), we have $\nu(b) = \nu(a)\psi(a)(s)$, whence $\nu(a) \preceq \nu(b)$ in M . Conversely, assume $\nu(a) \preceq \nu(b)$. Again, it is enough to consider the case $\nu(b) = \nu(a)s$ with s in S . Now, as $\psi(a)$ is bijective, there exists a unique r in S satisfying $\psi(a)(r) = s$, and, by (4.2), we have then $\nu(ar) = \nu(a)\psi(a)(r) = \nu(a)s = \nu(b)$, whence $b = ar$ since ν is injective, and $a \preceq b$ in $\mathbb{N}^{(S)}$.

(iii) The monoid $\mathbb{N}^{(S)}$ admits right-lcms, and (ii) enables us to transfer the result to M . So, let g, h belong to M . Put $a = \nu^{-1}(g)$ and $b = \nu^{-1}(h)$. Let ab' be the right-lcm of a and b in $\mathbb{N}^{(S)}$. By (ii), $\nu(ab')$ is a common right-multiple of g and h in M . Now, assume that f is a common right-multiple of g and h in M . By (ii) again, we have $a \preceq \nu^{-1}(f)$ and $b \preceq \nu^{-1}(f)$ in $\mathbb{N}^{(S)}$, whence $ab' \preceq \nu^{-1}(f)$. By (ii) once more, this implies $\nu(ab') \preceq f$ in M . So $\nu(ab')$ is a right-lcm of g and h in M , and M admits right-lcms. \square

We can now easily complete the proof of Proposition 4.3.

Proof of Proposition 4.3. Assume that ν is a right- I -structure on M , based on a set S . By Lemma 4.6(i), S must be the atom set of M , and the assumption that M is finitely generated implies that S is finite.

Next, the free Abelian monoid $\mathbb{N}^{(S)}$ satisfies the assumptions of Lemma 4.4 and, therefore, the latter applies. Hence, if we define $s * t = \psi(s)(t)$, then $(S, *)$ is an RC-quasigroup. Moreover, as S is finite, $(S, *)$ is bijective by [27, Theorem 2].

Assume $s \neq t \in S$. By (4.2), we have $s(s * t) = \nu(st) = \nu(ts) = t(t * s)$, whereas, by Lemma 4.6(i) and (iii), the monoid M admits unique right-lcms. Moreover, as S is finite, the argument of [25, Lemma 8.1.2(6)] shows that M must be left-cancellative (for that point we have no alternative method and it is useless to repeat the original argument, which easily adapts). It follows that $s(s * t)$ is necessarily the right-lcm of s and t , and we must have $s * t = s \setminus t$.

Finally, as M is left-cancellative, admits a length function, and admits right-lcms, and as S is the atom set of M , it follows from [8, Prop. 4.1] that the list of all relations $s(s \setminus t) = t(t \setminus s)$ with $s \neq t \in S$ make a presentation of M . By definition of $*$, this means that M is the structure monoid of $(S, *)$.

Finally, the connection between ν and the polynomials Π is given by the right formula in (4.6). The uniqueness of ν follows, as S is the atom set of M , and $*$ is the only possible extension of the right-complement operation outside the diagonal that admits bijective left-translations, so they only depend on M . \square

As observed in [24], (4.2) is reminiscent of a semi-direct product. For further reference, we now describe the connection formally, here in the slightly extended context of Lemma 4.4; the point is to have the formulas of (4.7) at hand.

Proposition 4.7. *Assume that M is a left-cancellative monoid, N is either \mathbb{N} or $\mathbb{Z}/d\mathbb{Z}$ for some d , and ν maps $N^{(S)}$ to M . Then the following are equivalent:*

- (i) *The map ν is a right- I -structure of shape $(N^{(S)}, S)$ on M ;*
- (ii) *There exists a map $\psi : N^{(S)} \rightarrow \mathfrak{S}_S$ such that $g \mapsto (\nu^{-1}(g), \psi(\nu^{-1}(g))^{-1})$ defines an injective homomorphism of M to the wreath product $N \wr \mathfrak{S}_S$ whose first component is a bijection.*

Proof. Assume that ν is a right I -structure of shape $N^{(S)}$ on M . Let ψ be the map from $N^{(S)}$ to \mathfrak{S}_S of (4.2). Define $\iota : M \rightarrow N \wr \mathfrak{S}_S$ by $\iota(g) = (\nu^{-1}(g), \psi(\nu^{-1}(g))^{-1})$, where $N \wr \mathfrak{S}_S$ is $N^{(S)} \rtimes \mathfrak{S}_S$ with \mathfrak{S}_S acting on $N^{(S)}$ by permuting positions.

First, ι is injective and its first component is bijective, since ν^{-1} is bijective.

In order to prove that (i) implies (ii), the point is to check that ι is a homomorphism. Let g, h belong to M . Putting $a = \nu^{-1}(g)$, $b = \nu^{-1}(h)$, $\sigma = \psi(a)$, and $\tau = \psi(b)$, we find $\iota(g) = (a, \sigma^{-1})$ and $\iota(h) = (b, \tau^{-1})$, whence, in $N \wr \mathfrak{S}_S$,

$$(4.9) \quad \iota(g)\iota(h) = (a\sigma^{-1}[b], \sigma^{-1} \circ \tau^{-1}).$$

On the other hand, the monoid $N^{(S)}$ satisfies (4.3), so Lemma 4.5 applies and, using the left formula in (4.7), we find

$$\nu(a\sigma^{-1}[b]) = \nu(a)\nu(\psi(a)(\sigma^{-1}[b])) = g\nu(\sigma[\sigma^{-1}[b]]) = g\nu(b) = gh,$$

whence $\nu^{-1}(gh) = a\sigma^{-1}[b]$. Using the right formula in (4.7) similarly, we find

$$\psi(a\sigma^{-1}[b]) = \psi(\psi(a)[\sigma^{-1}[b]]) \circ \psi(a) = \psi(\sigma[\sigma^{-1}[b]]) \circ \sigma = \psi[b] \circ \sigma = \tau \circ \sigma.$$

We deduce $\iota(gh) = (a\sigma^{-1}[b], \sigma^{-1} \circ \tau^{-1})$. So, by (4.9), ι is a homomorphism.

Conversely, assume (ii) with ν and ψ ensuring that ι is an embedding. Then the above computation gives, for all a, b in $N^{(S)}$, the equality $\nu(ab) = \nu(a)\nu(\psi(a)[b])$, whence in particular $\nu(as) = \nu(a)\psi(a)(s)$ for a in $N^{(S)}$ and s in S . So ν is a right- I -structure of shape $(N^{(S)}, S)$ on M , and (ii) implies (i) \square

5. COXETER-LIKE GROUPS

We now use the RC-calculus of Section 2 and the I -structure of Section 4 and to solve what can be called the quest of a Coxeter group, namely constructing for every group associated with a finite RC-quasigroup a finite quotient that plays the role played by Coxeter groups in the case of spherical Artin–Tits groups. This finite quotient is not the group G_X^0 of [16] in general.

In the case of Artin’s braid group B_n , the seminal example of a Garside group, the Garside structure (B_n^+, Δ_n) is connected with the symmetric group \mathfrak{S}_n . Precisely, the group B_n and the monoid B_n^+ admit the (Artin) presentation

$$(5.1) \quad \left\langle \sigma_1, \dots, \sigma_{n-1} \mid \begin{array}{ll} \sigma_i \sigma_j = \sigma_j \sigma_i & \text{for } |i - j| \geq 2 \\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j & \text{for } |i - j| = 1 \end{array} \right\rangle,$$

and \mathfrak{S}_n is the quotient of B_n obtained by adding the relations $\sigma_i^2 = 1$ to (5.1). Then there exists a set-theoretic section $\sigma : \mathfrak{S}_n \rightarrow B_n$ whose image is the family of all divisors of Δ_n in B_n^+ , and a presentation both of the group B_n and the monoid B_n^+ in terms of the image of σ consists of all relations $\sigma(f)\sigma(g) = \sigma(h)$ with f, g, h in \mathfrak{S}_n satisfying $\|f\| + \|g\| = \|h\|$, where $\|f\|$ is the length of f (minimal number of adjacent transpositions in a decomposition of f). Thus B_n appears as a sort of unfolded version of \mathfrak{S}_n where permutation length is used to get rid of torsion.

This is the situation we shall obtain in our current context. To make things precise, we introduce a notion of a Garside germ [13]. If a set S positively generates

a group G (that is, every element of G can be expressed as a product of elements of S), we denote by $\|g\|_S$ the length of a shortest S -decomposition of g .

Definition 5.1. If (M, Δ) is a Garside monoid and G is its group of fractions, a surjective homomorphism $\pi : G \rightarrow \overline{G}$ is said to *provide a Garside germ for (G, M, Δ)* if there exists a map $\sigma : \overline{G} \rightarrow M$ such that $\pi \circ \sigma$ is the identity, the image of σ is the family of all divisors of Δ in M , and M admits the presentation

$$(5.2) \quad \langle \sigma(\overline{G}) \mid \{\sigma(f)\sigma(g) = \sigma(fg) \mid f, g \in \overline{G} \text{ and } \|f\|_{\overline{S}} + \|g\|_{\overline{S}} = \|fg\|_{\overline{S}}\} \rangle,$$

where \overline{S} is the image under π of the atom set of M .

In the context of Definition 5.1, every element of G can be written as $\Delta^p g$ for some p in \mathbb{Z} and some g in M , implying that \overline{S} positively generates \overline{G} and making $\|g\|_{\overline{S}}$ meaningful. The term *germ* stems from [14, 13] where the germ derived from $(\overline{G}, \overline{S})$ is defined to be (\overline{G}, \bullet) where \bullet is the partial binary operation so that $f \bullet g = h$ holds for $fg = h$ with $\|f\|_{\overline{S}} + \|g\|_{\overline{S}} = \|h\|_{\overline{S}}$. The monoid and the group defined by (5.2) are then said to be generated by the germ (\overline{G}, \bullet) . The situation described in Definition 5.1 corresponds to (\overline{G}, \bullet) being a germ generating G . When it is so, the maps π and σ induce mutually inverse isomorphisms between the finite lattice made by the divisors of Δ in M and $(\overline{G}, \leq_{\overline{S}})$ where $f \leq_{\overline{S}} g$ means $\|f\|_{\overline{S}} + \|f^{-1}g\|_{\overline{S}} = \|g\|_{\overline{S}}$. The Hasse diagram of these partial orders then coincides with the Cayley graph of the germ (\overline{G}, \bullet) with respect to the generating set \overline{S} .

The above mentioned results for the braid group B_n and the symmetric group \mathfrak{S}_n can be summarized into the statement that collapsing σ_i^2 to 1 for every i provides a Garside germ for (B_n, B_n^+, Δ_n) , with associated quotient \mathfrak{S}_n . It is known—see [1] or [12, Chapter IX]—that similar results hold for every Artin–Tits group of spherical type: if (W, S) is a spherical Coxeter system (that is, W and S are finite), and G and M are the associated Artin–Tits group and monoid, and Δ is the right-lcm of atoms in M , then collapsing s^2 to 1 for every s in S provides a Garside germ for (G, M, Δ) , with associated quotient W .

It is then natural to ask whether similar results hold for every Garside group, namely whether some finite quotient provides a Garside germ, that is, in other words, whether there exists an associated Coxeter-like group enjoying all the nice properties known in the Artin–Tits case. No general answer is known, but we shall establish a complete positive answer for structure groups of finite RC-quasigroups. Indeed, we define for every finite RC-quasigroup a notion of *class* and prove:

Proposition 5.2. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d . Let G, M be the associated group and monoid, and Δ be the right-lcm of S in M . Then collapsing $s^{[d]}$ to 1 in G for every s in S , where $s^{[d]}$ stands for $\Pi_d(s, \dots, s)$, gives a finite group \overline{G} that provides a Garside germ for (G, M, Δ^{d-1}) . The group \overline{G} has d^n elements and the kernel of the projection is (isomorphic to) \mathbb{Z}^n .*

In the framework of Proposition 5.2, the finite group \overline{G} will be called the *Coxeter-like group* associated with $(S, *)$ and d .

The proof, which is not difficult, consists in using the I -structure to carry the results from the (trivial) case of \mathbb{Z}^n to the case of an arbitrary group of I -type. It will be decomposed into several easy steps. First we define the class.

Definition 5.3. An RC-quasigroup $(S, *)$ is said to be of *class d* if it satisfies

$$(5.3) \quad \forall s, t \in S \ (\ \Omega_{d+1}(s, \dots, s, t) = t \).$$

So an RC-quasigroup is of class 1 if $s * t = t$ holds for all s, t , and it is of class 2 if $(s * s) * (s * t) = t$ holds for all s, t .

Lemma 5.4. *Every RC-quasigroup of cardinal n is of class d for some $d < (n^2)!$.*

Proof. Let $(S, *)$ be a finite RC-quasigroup with cardinal n . By Rump's theorem, $(S, *)$ must be bijective, that is, the map $\Psi : (s, t) \mapsto (s * t, t * s)$ is bijective on $S \times S$. Consider $\Phi : (s, t) \mapsto (s * s, s * t)$ on S^2 . Assume $(s, t) \neq (s', t')$. For $s \neq s'$, we have $\Psi(s, s) \neq \Psi(s', s')$, hence $s * s \neq s' * s'$, and $\Phi(s, t) \neq \Phi(s', t')$. For $s = s'$, we must have $t \neq t'$, whence $s * t \neq s * t'$ and, again, $\Phi(s, t) \neq \Phi(s', t')$ since left-translations of $*$ are injective. So Φ is injective, hence bijective on the finite set $S \times S$. As $S \times S$ has cardinal n^2 , the order of Φ in $\mathfrak{S}_{S \times S}$ is at most $(n^2)!$. So there exists $d < (n^2)!$ such that Φ^{d+1} is the identity. Now, an easy induction gives $\Phi^m(s, t) = (\Omega_m(s, \dots, s, s), \Omega_m(s, \dots, s, t))$ for every m . So $\Phi^{d+1} = \text{id}$ implies $\Omega_{d+1}(s, \dots, s, t) = t$ for all s, t in S . \square

There exist finite RC-quasigroups with an arbitrarily high minimal class. Indeed, let $S = \{\mathbf{a}_1, \dots, \mathbf{a}_n\}$ and $s * t = f(t)$ where f maps \mathbf{a}_i to $\mathbf{a}_{i+1 \pmod n}$ for every i . Then, for all p, i and s_1, \dots, s_p in S , we have $\Omega_{p+1}(s_1, \dots, s_p, \mathbf{a}_i) = \mathbf{a}_{i+p \pmod n}$. Hence $(S, *)$ is of class d if and only if d is a multiple of n , and the minimal class is n .

We shall establish Proposition 5.2 using the I -structure on the monoid M , which exists by Proposition 4.2. As in Section 4, the I -structure will be denoted by ν , and the associated map from \mathbb{N}^S to \mathfrak{S}_S as defined in (4.2) will be denoted by ψ . As mentioned at the end of Section 4, ν and ψ respectively extend into a bijection from \mathbb{Z}^S to G and a map from \mathbb{Z}^S to \mathfrak{S}_S that still satisfy (4.1) and (4.2).

Lemma 5.5. *Assume that $(S, *)$ is an RC-quasigroup of class d and M is the associated monoid. For s in S and $q \geq 0$, let $s^{[q]} = \Pi_q(s, \dots, s)$. Then $\nu(s^d a) = s^{[d]} \nu(a)$ holds for all s in S and a in $\mathbb{N}^{(S)}$. The permutation $\psi(s^d)$ is the identity and, for all s, t in S , the elements $s^{[d]}$ and $t^{[d]}$ commute in M .*

Proof. Assume $a = t_1 \dots t_q$ with t_1, \dots, t_q in S . Proposition 4.2 implies

$$\begin{aligned} \nu(s^d a) &= \Pi_{d+q}(s, \dots, s, t_1, \dots, t_q) \\ &= \Pi_d(s, \dots, s) \Pi_q(\Omega_{d+1}(s, \dots, s, t_1), \dots, \Omega_{d+1}(s, \dots, s, t_q)) \\ &= \Pi_d(s, \dots, s) \Pi_q(t_1, \dots, t_q) = \nu(s^d) \nu(t_1 \dots t_q) = s^{[d]} \nu(a), \end{aligned}$$

in which the second equality comes from expanding the terms and the third one from the assumption that M is of class d . Applying with $a = t$ in S and merging with $\nu(s^d t) = \nu(s^d) \psi(s^d)(t)$, we deduce that $\psi(s^d)$ is the identity. On the other hand, applying with $a = t^{[d]}$, we find $s^{[d]} t^{[d]} = \nu(s^d t^d) = \nu(t^d s^d) = t^{[d]} s^{[d]}$. \square

Lemma 5.6. (i) *Assume that $(S, *)$ is a finite RC-quasigroup, M is the associated monoid, and $d \geq 2$ holds. Let $\Delta_\bullet = \prod_{s \in S} s$ in \mathbb{N}^S and $\Delta_d = \nu(\Delta_\bullet^{d-1})$. Then we have $\Delta_d = \Delta^{d-1}$ where Δ is the right-lcm of S , and Δ_d is a Garside element in M .*

(ii) *If, moreover, $(S, *)$ is of class d , then Δ^d and $(\Delta_d)^d$ lie in the centre of M .*

Proof. (i) By Lemma 3.3, we have $\Delta = \Pi_n(s_1, \dots, s_n) = \nu(\Delta_\bullet)$, where (s_1, \dots, s_n) is any enumeration of S . In other words, we have $\Delta = \Delta_2$. Now, we observe that $f[\Delta_\bullet] = \Delta_\bullet$ holds in \mathbb{N}^S for every f in \mathfrak{S}_S since every element of S occurs once in the definition of Δ_\bullet . By (4.7), we deduce

$$(5.4) \quad \nu(a \Delta_\bullet) = \nu(a) \nu(\psi(a)[\Delta_\bullet]) = \nu(a) \nu(\Delta_\bullet),$$

whence $\nu(\Delta_{\bullet}^k) = \nu(\Delta_{\bullet})^k$ for every k and, in particular, $\Delta_d = \nu(\Delta_{\bullet})^{d-1} = \Delta^{d-1}$. By Proposition 3.5, Δ is a Garside element in M . It is standard that this implies that every power of Δ is also a Garside element, hence, in particular, so is Δ_d .

(ii) Assume now that $(S, *)$ is of class d . Let t belong to S . Then, by (5.4), we obtain $\nu(t\Delta_{\bullet}^d) = \nu(t)\nu(\Delta_{\bullet}^d) = t\Delta^d$. On the other hand, (5.4) and Lemma (5.5) give

$$(5.5) \quad \Delta^d = \nu(\Delta_{\bullet}^d) = \prod_{s \in S} s^{[d]} \text{ and } \nu(\Delta_{\bullet}^d t) = \prod_{s \in S} s^{[d]} t = \Delta^d t.$$

Merging the values of $\nu(t\Delta_{\bullet}^d)$ and $\nu(\Delta_{\bullet}^d t)$, we obtain $t\Delta^d = \Delta^d t$, so that Δ^d , hence its power $(\Delta_d)^d$ as well, lies in the centre of M . \square

We can now introduce the equivalence relation on \mathbb{Z}^S that, when carried to G , induces the expected quotient of G (and M). For a in \mathbb{Z}^S , we denote by $\#_s(a)$ the (well-defined) algebraic number of letters s in any S -decomposition of a .

Lemma 5.7. *Assume that $(S, *)$ is an RC-quasigroup of class d and M and G are the associated monoid and group. For a, a' in \mathbb{Z}^S , write $a \equiv_{\bullet} a'$ if $\#_s(a) \equiv \#_s(a') \pmod{d}$ holds for every s in S .*

(i) *For g, g' in M , declare $g \equiv g'$ for $\nu^{-1}(g) \equiv_{\bullet} \nu^{-1}(g')$. Then \equiv is an equivalence relation on M that is compatible with left- and right-multiplication. The class of 1 is the Abelian submonoid M_1 of M generated by the elements $s^{[d]}$ with s in S .*

(ii) *For g, g' in G , declare that $g \equiv g'$ holds if there exist h, h' in M and r, r' in \mathbb{Z} satisfying $g = \Delta^{dr}h$, $g' = \Delta^{dr'}h'$, and $h \equiv h'$. Then \equiv is a congruence on G , and the kernel of the projection of G to G/\equiv is the group of fractions of M_1 .*

Proof. (i) As ν is bijective, carrying the equivalence relation \equiv_{\bullet} of \mathbb{N}^S to M yields an equivalence relation on M . Assume $g \equiv g'$. Let $a = \nu^{-1}(g)$ and $a' = \nu^{-1}(g')$. Without loss of generality, we may assume $a' = as^d = s^d a$ for some s in S . Applying (4.7) and Lemma 5.5, we obtain $\psi(a') = \psi(\psi(s^d)[a]) \circ \psi(s^d) = \psi(a)$. Let t belong to S . Using (4.7) again, we deduce

$$\begin{aligned} g \cdot \psi(a)(t) &= \nu(a) \cdot \psi(a)(t) = \nu(at) \\ &\equiv \nu(a't) = \nu(a') \cdot \psi(a')(t) = \nu(a') \cdot \psi(a)(t) = g' \cdot \psi(a)(t). \end{aligned}$$

As $\psi(a)(t)$ takes every value in S when t ranges over S , we deduce that \equiv is compatible with right-multiplication. On the other hand, $a \equiv_{\bullet} a'$ implies $f[a] \equiv_{\bullet} f[a']$ for every permutation f of S . Let t belong to S . Always by (4.7), we obtain

$$t \cdot g = t \cdot \nu(a) = \nu(t \cdot \psi(t)^{-1}[a]) \equiv \nu(t \cdot \psi(t)^{-1}[a']) = t \cdot \nu(a') = t \cdot g',$$

and \equiv is compatible with left-multiplication by S .

The \equiv_{\bullet} -class of 1 in \mathbb{N}^S is the free Abelian submonoid generated by the elements s^d with s in S . The \equiv -class of 1 in M consists of the ν -image of the products of such elements s^d . By Lemma 5.5, the latter are the products of elements $s^{[d]}$.

(ii) First, \equiv is well-defined. As Δ^d is a Garside element in M , every element of G admits an expression $\Delta^{dr}h$ with r in \mathbb{Z} and h in M . This expression is not unique, but, if we have $g = \Delta^{dr}h = \Delta^{dr_1}h_1$ with, say, $r_1 < r$, then, as M is left-cancellative, we must have $h_1 = \Delta^{d(r-r_1)}h$, whence $h_1 \equiv h$ by (5.5). So, for every h' in M , the relations $h \equiv h'$ and $h_1 \equiv h'$ are equivalent.

That \equiv is an equivalence relation is easy. Its compatibility with multiplication on G follows from the compatibility on M and the fact that Δ^d is central in G .

Finally, the \equiv -class of 1 in G consists of all elements $\Delta^{dr}h$ with h in M_1 . As Δ^d belongs to M_1 , this is the group of fractions of M_1 in G , hence the free Abelian subgroup of G generated by the elements $s^{[d]}$ with s in S . \square

Proof of Proposition 5.2. Let \overline{G} be the quotient-group G/\equiv . By Lemma 5.7, the kernel of the projection of G onto \overline{G} is a free Abelian group of rank n , hence it is isomorphic to \mathbb{Z}^S . The cardinality of \overline{G} is the number of \equiv -classes in G . As every element of G is \equiv -equivalent to an element of M , this number is also the number of \equiv -classes in M , hence the number d^n of \equiv_\bullet -classes in \mathbb{N}^S , and we have $\overline{G} = M/\equiv$.

By definition, $s^{[d]} \equiv 1$ holds for s in S . Conversely, the congruence \equiv_\bullet on \mathbb{Z}^S is generated by the pairs $(s^d, 1)$ with s in S , hence the congruence \equiv on G is generated by the pairs $(s^{[d]}, 1)$ with s in S . Hence a presentation of \overline{G} is obtained by adding to the presentation (1.10) of G and of M the n relations $s^{[d]} = 1$ with s in S .

By construction, the bijection ν is compatible with the congruences \equiv_\bullet on \mathbb{Z}^S and \equiv on G , so it induces a bijection $\overline{\nu}$ of $\mathbb{N}^S/\equiv_\bullet$, which is $(\mathbb{Z}/d\mathbb{Z})^S$, onto M/\equiv , which is \overline{G} , providing a commutative diagram

$$(5.6) \quad \begin{array}{ccc} \mathbb{N}^S & \xrightarrow{\nu} & M \\ \pi_\bullet \downarrow & & \downarrow \pi \\ (\mathbb{Z}/d\mathbb{Z})^S & \xrightarrow{\overline{\nu}} & \overline{G} \end{array}$$

Now, let σ_\bullet be the section of π_\bullet from $(\mathbb{Z}/d\mathbb{Z})^S$ to \mathbb{N}^S that maps every \equiv_\bullet -class to the unique n -tuple of $\{0, \dots, d-1\}^S$ that lies in that class, and let $\sigma : \overline{G} \rightarrow M$ be defined by $\sigma(g) = \nu(\sigma_\bullet(\overline{\nu}^{-1}(g)))$. Then, for every g in \overline{G} , we obtain

$$\pi(\sigma(g)) = \pi(\nu(\sigma_\bullet(\overline{\nu}^{-1}(g))) = \overline{\nu}(\pi_\bullet(\sigma_\bullet(\overline{\nu}^{-1}(g))) = g$$

since σ_\bullet is a section of π_\bullet . Hence σ is a section of π . Next, by construction, the image of \overline{G} under σ is the image under ν of $\{0, \dots, d-1\}^S$, hence the image under ν of the family of all left-divisors of Δ_\bullet^{d-1} in \mathbb{N}^S , hence the family of all left-divisors of Δ^{d-1} , that is, of Δ_d , in M .

Finally, the relation $\sigma(f)\sigma(g) = \sigma(fg)$ holds in M if and only if the relation $\sigma_\bullet(\overline{\nu}(f))\sigma_\bullet(\overline{\nu}(g)) = \sigma_\bullet(\overline{\nu}(fg))$ holds in \mathbb{N}^S , hence if and only if, for every i , the sum of the i th coordinates of $\overline{\nu}(f)$ and $\overline{\nu}(g)$ does not exceed $d-1$. This happens if and only if $\|\overline{\nu}(f)\|_S + \|\overline{\nu}(g)\|_S = \|\overline{\nu}(fg)\|_S$ holds in $(\mathbb{Z}/d\mathbb{Z})^S$, hence if and only if $\|f\|_{\overline{G}} + \|g\|_{\overline{G}} = \|fg\|_{\overline{G}}$ holds in \overline{G} . By construction, the family S is included in the image of σ , and all length two relations of (1.10) belong to the previous list of relations, hence the latter make a presentation of M . This completes the proof. \square

Example 5.8. For an RC-quasigroup of class 1, that is, satisfying $s * t = t$ for all s, t , the group G is a free Abelian group, \overline{G} is trivial, and Proposition 5.2 here reduces to the isomorphism $\mathbb{Z}^S \cong G$.

For class 2, that is, when $(s * s) * (s * t) = t$ holds for all s, t , the element Δ_d is the right-lcm of S , it has 2^n divisors which are the right-lcms of subsets of S , and the group \overline{G} is the order 2^n quotient of G obtained by adding the relations $s(s * s) = 1$. For instance, in the case of $\{\mathbf{a}, \mathbf{b}\}$ with $s * t = f(t)$, $f : \mathbf{a} \mapsto \mathbf{b} \mapsto \mathbf{a}$, the group G has the presentation $\langle \mathbf{a}, \mathbf{b} \mid \mathbf{a}^2 = \mathbf{b}^2 \rangle$, the relations $\mathbf{a}^{[2]} = \mathbf{b}^{[2]} = 1$ both amount to $\mathbf{ab} = 1$, and the associated Coxeter-like group \overline{G} is a cyclic group of order 4.

For class 3, let us consider as in Example 3.6 the RC-quasigroup $\{\mathbf{a}, \mathbf{b}, \mathbf{c}\}$ with $s * t = f(t)$ and $f : \mathbf{a} \mapsto \mathbf{b} \mapsto \mathbf{c} \mapsto \mathbf{a}$. The presentation of the associated group G

is $\langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2 \rangle$. With the same notation as above, the smallest Garside element Δ is a^3 . As the class of $(S, *)$ is 3, we consider here $\Delta_3 = \Delta^2 = a^6$. The lattice $\text{Div}(\Delta_3)$ has 27 elements, its Hasse diagram is the cube shown in Figure 3. The latter is also the Cayley graph of the germ derived from $(\overline{G}, \{a, b, c\})$, that is, the restriction of the Cayley graph of \overline{G} to the partial product of the germ. Adding to the above presentation the relations $s^{[3]} = 1$, that is, $s(s * s)((s * s) * (s * s)) = 1$, namely $abc = bca = cab = 1$, here reducing to $abc = 1$, yields for \overline{G} the presentation $\langle a, b, c \mid ac = b^2, ba = c^2, cb = a^2, abc = 1 \rangle$. One can check that other presentations of \overline{G} are $\langle a, b \mid a = b^2ab, b = aba^2 \rangle$ and $\langle a, b \mid a = b^2ab, a^3 = b^3 \rangle$.

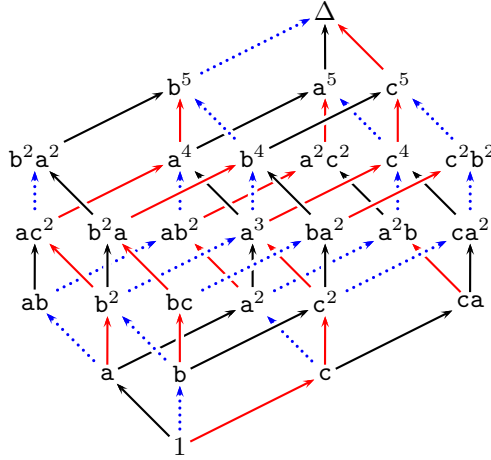


FIGURE 3. The Coxeter-like group associated with the RC-quasigroup of Example 3.6; the 27-vertex cube shown above is the lattice of divisors of a^6 in the associated monoid M , the Hasse diagram of the weak order on the finite group \overline{G} with respect to the generators a, b, c , and the Cayley graph of the germ derived from \overline{G} with respect to the previous generators. The complete Cayley graph of \overline{G} would be obtained by adding arrows that correspond to cases when the S -lengths do not add, for instance $ab \cdot c = 1$, as when one transforms a cube into a 3-torus by gluing opposite faces.

Remark 5.9. (i) General results by Gromov imply that every finitely generated group G whose Cayley graph is (quasi)-isometric to that of \mathbb{Z}^n must be virtually \mathbb{Z}^n , that is, there exists an exact sequence $1 \rightarrow \mathbb{Z}^n \rightarrow G \rightarrow \overline{G} \rightarrow 1$ with \overline{G} finite, see [2]. By definition, an I -structure is an isometry as above, and the existence of a finite quotient \overline{G} as in Proposition 5.2 can be seen as a concrete instance of the above (abstract) result.

(ii) In [16], one considers the quotient $G_S^0 = G/\Gamma$, where Γ consists of the elements whose action on S is trivial. By Lemma 5.5, $\psi(s^d)$ is the identity permutation for every s in S , meaning that every element $s^{[d]}$ belongs to Γ . Hence G_S^0 is a quotient of our current group \overline{G} , a proper one in general: for the groups of Example 5.8, in the class 2 example, the orders of G_S^0 and \overline{G} are 2 vs. 4 (ab lies in Γ but it is not trivial in \overline{G}), in the class 3 example, the orders are 3 vs. 27.

The question naturally arises of characterizing Coxeter-like groups associated with finite RC-quasigroups (hence, equivalently, with solutions of YBE) as described

in Proposition 5.2. We show now that, exactly as structure groups of solutions of YBE are those groups that admit an I -structure, their Coxeter-like quotients are those finite groups that admit the counterpart of an I -structure where some cyclic group $\mathbb{Z}/d\mathbb{Z}$ replaces \mathbb{Z} , that is, what was called an I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$ in Definition 4.1.

Proposition 5.10. *For every finite group W , the following are equivalent:*

- (i) *There exists a finite RC-quasigroup $(S, *)$ of class d such that W is the Coxeter-like group associated with $(S, *)$ and d .*
- (ii) *The group W admits a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$.*

Proof. Assume that $(S, *)$ is a finite RC-quasigroup and G and M are the associated group and monoid. Then M admits an I -structure ν . The congruences of Lemma 5.7, \equiv_\bullet on \mathbb{Z}^S and \equiv on G , are compatible and ν induces a well-defined map $\bar{\nu}$ from $(\mathbb{Z}/d\mathbb{Z})^S$ to G/\equiv that makes (5.6) commutative. Then $\bar{\nu}$ is bijective by construction, and projecting (4.2) for ν gives its counterpart for $\bar{\nu}$. So $\bar{\nu}$ is a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$ for G/\equiv , and (i) implies (ii).

Conversely, assume that W admits a right- I -structure of shape $(\mathbb{Z}/d\mathbb{Z})^S$. As $(\mathbb{Z}/d\mathbb{Z})^S$ satisfies (4.3), Lemmas 4.4 and 4.5 apply. Thus putting $s * t = \psi(s)(t)$ yields an RC-quasigroup and (4.6) is valid. Let s and t belong to S . In $(\mathbb{Z}/d\mathbb{Z})^S$, we have $s^d = 1$, whence $\psi(s^d) = \psi(1) = \text{id}_S$. Applying (4.6) (left), we deduce $\Omega_{d+1}(s, \dots, s, t) = \psi(s^d)(t) = t$. Hence the RC-quasigroup $(S, *)$ is of class d .

Now, let G be the group associated with $(S, *)$, and let \bar{G} be the associated finite quotient as provided by Proposition 5.2. The group G is generated by S and it admits a presentation consisting of all relations $s(s * t) = t(t * s)$ with s, t in S . By assumption, the group W is generated by S , and we observed that the relations $s(s * t) = t(t * s)$ with s, t in S are satisfied in W since, by definition, they are equivalent to $\nu(st) = \nu(ts)$ and $(\mathbb{Z}/d\mathbb{Z})^S$ is Abelian. Hence there exists a surjective homomorphism θ from G to W that is the identity on S .

$$\begin{array}{ccccc}
 \mathbb{Z}^S & \xrightarrow{\hat{\nu}} & G & & \\
 \pi_\bullet \downarrow & & \downarrow \pi & \searrow \theta & \\
 (\mathbb{Z}/d\mathbb{Z})^S & \xrightarrow{\quad} & \bar{G} & \xrightarrow{\bar{\theta}} & W \\
 & \searrow \nu & & &
 \end{array}$$

Next, \bar{G} is the quotient of G obtained by adding the relations $s^{[d]} = 1$, that is, $\Pi_d(s, \dots, s) = 1$ for s in S . Now, in W , we have $\Pi_d(s, \dots, s) = \nu(s^d)$ by (4.6); but $s^d = 1$ holds in $(\mathbb{Z}/d\mathbb{Z})^S$, so, in W , we have $\Pi_d(s, \dots, s) = 1$ for every s in S . Thus the surjective homomorphism θ factorizes through \bar{G} , yielding a surjective homomorphism $\bar{\theta}$ from \bar{G} to W . As both \bar{G} and W have cardinality d^n , the homomorphism $\bar{\theta}$ must be an isomorphism. Hence W is the Coxeter-like quotient of the group associated with $(S, *)$ and d . So (ii) implies (i). \square

Using Proposition 4.7, we deduce

Corollary 5.11. *Every finite group that is the Coxeter-like group associated with an RC-quasigroup of size n and class d embeds into the wreath product $(\mathbb{Z}/d\mathbb{Z}) \wr \mathfrak{S}_n$ so that the first component is a bijection.*

Example 5.12. For the last group \bar{G} of Example 5.8, owing to the fact that the permutations of $\{1, 2, 3\}$ associated with $\mathbf{a}, \mathbf{b}, \mathbf{c}$ all are the cycle $f : 1 \mapsto 2 \mapsto 3 \mapsto 1$,

one obtains a description as the family of the 27 tuples $(p, q, r; f^{p+q+r})$ with p, q, r in $\mathbb{Z}/3\mathbb{Z}$, the product of triples being twisted by the action of f^{p+q+r} on positions.

Corollary 5.11 implies that the Coxeter-like groups \overline{G} associated with finite RC-quasigroups are IG -monoids in the sense of [23]. It follows that they inherit all properties of such monoids established there, in particular in terms of the derived algebras $K[\overline{G}]$ and their prime ideals.

We conclude with linear representations of the groups G and \overline{G} associated with a finite RC-quasigroup. Here again, we use the I -structure to carry the results from the trivial case of a free Abelian group to the group of an arbitrary RC-quasigroup.

Proposition 5.13. *Assume that $(S, *)$ is an RC-quasigroup of cardinal n and class d . Let G be the associated group. For s the i th element of S , define*

$$(5.7) \quad \Theta(s) = \Theta_{\bullet}(s) P_{\psi(s)},$$

where $\Theta_{\bullet}(s)$ is the diagonal $n \times n$ -matrix with diagonal entries $(1, \dots, 1, q, 1, \dots, 1)$, q at position i and $P_{\psi(s)}$ is the permutation matrix associated with $\psi(s) : t \mapsto s * t$. Then Θ provides a faithful representation of G into $\mathrm{GL}(n, \mathbb{Q}[q, q^{-1}])$; specializing at $q = \exp(2i\pi/d)$ gives a faithful representation of the associated group \overline{G} .

Proof. First, Θ_{\bullet} defines a faithful representation of \mathbb{Z}^S into $\mathrm{GL}(n, \mathbb{Q}[q, q^{-1}])$ since $\Theta_{\bullet}(\prod \mathbf{s}_i^{e_i})$ is the diagonal matrix with diagonal $(q^{e_1}, \dots, q^{e_n})$, and specializing at $q = \exp(2i\pi/d)$ gives a faithful representation of $(\mathbb{Z}/d\mathbb{Z})^S$.

In order to carry the results to G and \overline{G} , we show that (5.7) extends into $\Theta(\nu(a)) = \Theta_{\bullet}(a) P_{\psi(a)}$ for every a in \mathbb{Z}^S . As we are working with invertible matrices, it is enough to consider multiplication by one element of S (division automatically follows) and, therefore, the point for an induction is to go from a to as . We find

$$\begin{aligned} \Theta(\nu(as)) &= \Theta(\nu(a)\psi(a)(s)) && \text{by (4.2)} \\ &= \Theta(\nu(a)) \Theta(\psi(a)(s)) && \text{by definition} \\ &= \Theta_{\bullet}(a) P_{\psi(a)} \Theta_{\bullet}(\psi(a)(s)) P_{\psi(\psi(a)(s))} && \text{by induction hypothesis} \\ &= \Theta_{\bullet}(a) \Theta_{\bullet}(s) P_{\psi(a)} P_{\psi(\psi(a)(s))} && \text{by conjugating by } P_{\psi(a)} \\ &= \Theta_{\bullet}(as) P_{\psi(\psi(a)(s)) \circ \psi(a)} && \text{by definition} \\ &= \Theta_{\bullet}(as) P_{\psi(as)}. && \text{by (4.7)} \end{aligned}$$

It is then clear that Θ is well-defined on the monoid associated with $(S, *)$, hence on its group of fractions, which is G . For faithfulness, $\Theta_{\bullet}(\nu^{-1}(g))$ is the unique diagonal matrix obtained from $\Theta(g)$ by right-multiplication by a permutation matrix, so $\Theta(g)$ determines $\nu^{-1}(g)$, hence g .

Finally, specializing at a d th root of unity induces a well-defined faithful representation of the finite group \overline{G} since, by definition, g and g' represent the same element of \overline{G} if and only if $\nu^{-1}(g)$ and $\nu^{-1}(g')$ are \equiv_{\bullet} -equivalent, hence if and only if $\Theta_{\bullet}(\nu^{-1}(g))_{q=\exp(2i\pi/d)}$ and $\Theta_{\bullet}(\nu^{-1}(g'))_{q=\exp(2i\pi/d)}$ are equal. \square

Example 5.14. Coming back to the last group in Example 5.8, the permutations $\psi(\mathbf{a})$, $\psi(\mathbf{b})$, $\psi(\mathbf{c})$ all are the 3-cycle $(1, 2, 3)$, and we find the explicit representation

$$\Theta(\mathbf{a}) = \begin{pmatrix} 0 & q & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad \Theta(\mathbf{b}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & q \\ 1 & 0 & 0 \end{pmatrix}, \quad \Theta(\mathbf{c}) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ q & 0 & 0 \end{pmatrix}.$$

Specializing at $q = \exp(2i\pi/3)$ gives a faithful unitary representation of the associated 27-element group \overline{G} . Using the latter, it is easy to check for instance that \overline{G} has exponent 9: a, b, c have order 9, and all elements have order 1, 3, or 9.

Corollary 5.15. *Every finite group that is the Coxeter-like group associated with an RC-quasigroup of size n can be realized as a group of isometries in an n -dimensional Hermitian space.*

Indeed, the matrices $\Theta_\bullet(s)_{q=\exp(2i\pi/d)}$ correspond to order d complex reflections, whereas permutation matrices are finite products of hyperplane symmetries.

We shall not go farther in the description of the Coxeter-like groups \overline{G} . The analogy with Coxeter groups suggests to further investigate their geometric properties: according to Proposition 5.10 and Figure 3, the Cayley graph of the Coxeter-like group associated with an RC-quasigroup of cardinal n and class d is drawn on an n -torus and corresponds to a tiling of the torus (hence to a periodic tiling of \mathbb{R}^n) by d^n copies of a single cubical pattern. On the other hand, as \overline{G} characterizes the RC-quasigroup it comes from, classifying all finite groups (or all periodic tilings of \mathbb{R}^n) that occur in this way is *a priori* not easier than classifying all solutions of YBE, hence presumably (very) difficult.

We conclude with a speculative idea. So far, Propositions 3.7 and 4.2 provide the only known characterization of a relatively large family of Garside groups: it identifies Garside groups that admit a presentation of a certain form with those that admit an I -structure, hence resemble a free Abelian group. One might replace free Abelian groups with other groups Γ and consider as in [23] those groups G that admit a “ I -structure of shape Γ ” in the sense that their Cayley graph is that of Γ up to relabeling the edges. Should this approach make sense here, a natural problem would be to characterize those Garside groups that admit an I -structure of shape Γ for various reference (Garside) groups Γ , maybe a first step toward a global classification of Garside groups which, so far, remains out of reach.

REFERENCES

- [1] N. Bourbaki, *Groupes et algèbres de Lie*, chapitres I–III, Masson, Paris (1972).
- [2] M.R. Bridson and S.M. Gersten, *The optimal isoperimetric inequality for torus bundles over the circle*, Quart. J. Math. Oxford **47** (1996) 1–23.
- [3] F. Cedó, E. Jespers, and Á. del Río, *Involutive Yang-Baxter groups*, Trans. Amer. Math. Soc. **362** (2010) 2541–2558.
- [4] F. Cedó, E. Jespers, and J. Okniński, *Braces and the Yang-Baxter equation*, Comm. Math. Physics **327** (2014) 101–116; arXiv:1205.3587.
- [5] F. Chouraqui, *Garside groups and Yang-Baxter equations*, Comm. Algebra **38-12** (2010) 4441–4460.
- [6] F. Chouraqui and E. Godelle, *Finite quotients of groups of I-type*, Adv. in Math., to appear; arXiv:1301.3707.
- [7] A.H. Clifford and G.B. Preston, *The algebraic Theory of Semigroups*, vol. 1, Amer. Math. Soc. Surveys **7**, (1961).
- [8] P. Dehornoy and L. Paris, *Gaussian groups and Garside groups, two generalizations of Artin groups*, Proc. London Math. Soc. **79-3** (1999) 569–604.
- [9] P. Dehornoy, *Groupes de Garside*, Ann. Scient. Ec. Norm. Sup. **35** (2002) 267–306.
- [10] P. Dehornoy, *Complete positive group presentations*, J. of Algebra **268** (2003) 156–197.
- [11] P. Dehornoy, *The group of fractions of a torsion free lcm monoid is torsion free*, J. Algebra **281** (2004) 303–305.
- [12] P. Dehornoy, with F. Digne, E. Godelle, D. Krammer, J. Michel, *Foundations of Garside Theory*, EMS Tracts in Mathematics, to appear; www.math.unicaen.fr/~garside/Garside.pdf.

- [13] P. Dehornoy, F. Digne, and J. Michel, *Garside families and Garside germs*, J. of Algebra **380** (2013) 109145.
- [14] F. Digne and J. Michel, *Garside and locally Garside categories*, Preprint; math.GR/0612652.
- [15] V.G. Drinfeld, *On unsolved problems in quantum group theory*, Quantum Groups, Lecture Notes in Math. 1510, Springer-Verlag, Berlin, 1992, 1–8.
- [16] P. Etingof, T. Schedler, and A. Soloviev, *Set-theoretical solutions to the quantum Yang-Baxter equation*, Duke Math. J. **100** (1999) 169–209.
- [17] R. Fenn, M. Jordan-Santana, and L. Kauffman, *Biquandles and virtual links*, Topology and its Applic. **145** (2004) 157–175.
- [18] R. Fenn and C.P. Rourke, *Racks and links in codimension 2*, J. Knot Theory and its Ramifications **1-4** (1992) 343–406;
- [19] T. Gateva-Ivanova, *Garside structures on monoids with quadratic square-free relations*, Algebr. Represent. Theory **14** (2011) 779–802.
- [20] T. Gateva-Ivanova and M. Van den Bergh, *Semigroups of I-type*, J. Algebra **206** (1998) 97–112.
- [21] T. Gateva-Ivanova and S. Majid, *Set theoretic solutions of the Yang-Baxter equation, graphs and computations*, J. Symbolic Comput. **42** (2007) 1079–1112.
- [22] T. Gateva-Ivanova and S. Majid, *Matched pairs approach to set theoretic solutions of the Yang-Baxter equation*, J. Algebra **319** (2008) 1462–1529.
- [23] I. Goffa and E. Jespers, *Monoids of IG-type and maximal orders*, J. Algebra; 308; 2007; 44–62.
- [24] E. Jespers and J. Okniński, *Monoids and groups of I-type*, Algebr. Represent. Theory; 8; 2005; 709–729.
- [25] E. Jespers and J. Okniński, *Noetherian semigroup algebras*, Algebra and Applications vol. 7, Springer-Verlag (2007).
- [26] M. Jimbo, *Introduction to the Yang-Baxter equation*, Int. J. Modern Physics A **4-15** (1989) 3759–3777.
- [27] W. Rump, *A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation*, Adv. in Math. **193** (2005) 40–55.
- [28] W. Rump, *Modules over braces*, Algebra Discrete Math. **2** (2006) 127–137.
- [29] W. Rump, *Braces, radical rings, and the quantum Yang-Baxter equation*, J. Algebra **307** (2007) 153–170.

LABORATOIRE DE MATHÉMATIQUES NICOLAS ORESME, UMR 6139 CNRS, UNIVERSITÉ DE CAEN
BP 5186, 14032 CAEN CEDEX, FRANCE

Current address: LABORATOIRE PREUVES, PROGRAMMES, SYSTÈMES, UMR 7126 CNRS, UNI-
VERSITÉ PARIS-DIDEROT CASE 7014, 75205 PARIS CEDEX 13, FRANCE

E-mail address: `dehornoy@math.unicaen.fr`

URL: `//www.math.unicaen.fr/~dehornoy`